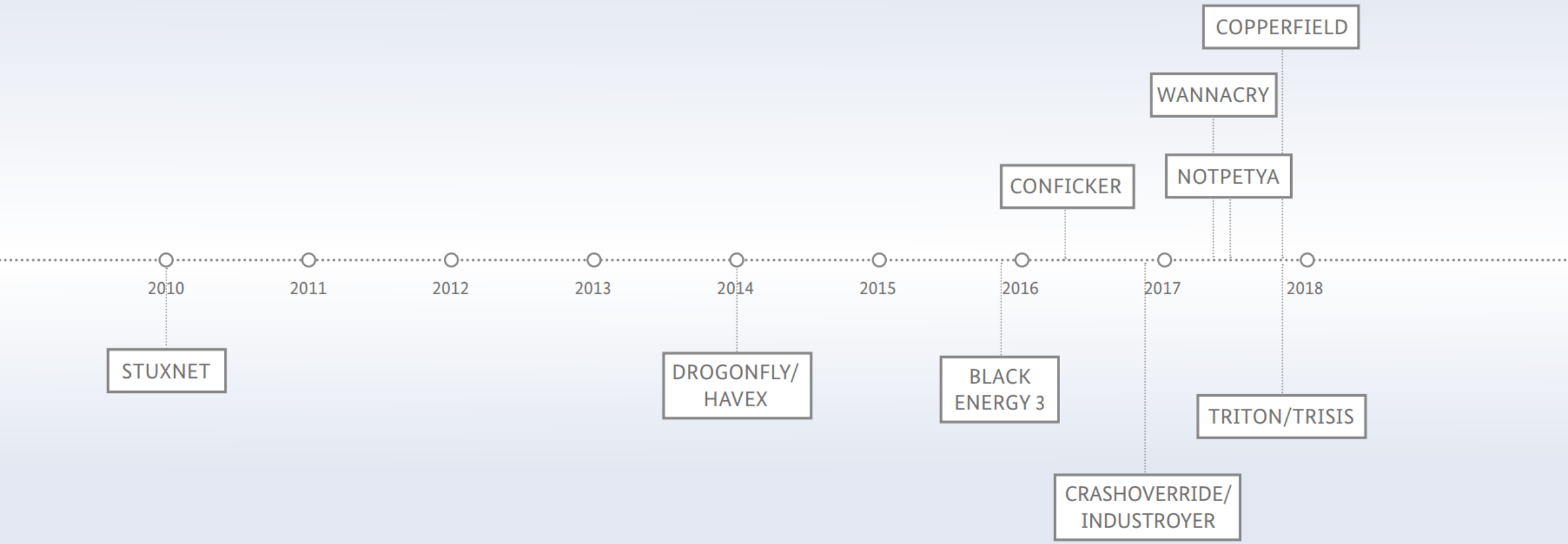
Кибербезопасность АСУ ТП

Средства и методы снижение рисков в системах промышленной автоматики

serhii.stepaniuk@siemens.com

Временная шкала ТОП целевых и не целевых атак, затронувших АСУ

SIEMENS
Ingenuity for life



https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2018-01.pdf?__blob=publicationFile&v=5

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

Вызовы сходные, но реальность существенно различна в IT и промышленной (OT) безопасности

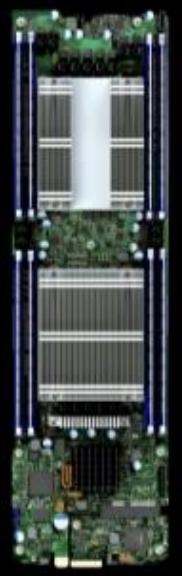
SIEMENS
Ingenuity for life

IT безопасность		Промышленная безопасность
Конфиденциальность		**Доступность**
3-5 гот	**Жизненный цикл активов**	20-40 лет
Принудит. миграция (ПК, смартфоны)	**Жизненный цикл** Аппаратуры	Использование пока доступны запчасти
Высокая (> 10 “агнетов” на офисном ПК)	**Возможности добавить ПО**	Низкая (старые системы, нет “свободных” ресурсов)
Низкая (~2 поколения, Windows 7 и 10)	**Неоднородность**	Высокая (от Windows 95 до 10)
По стандарту (агенты и принуд.обновлени	**Основная концепция защиты**	По случаю и по риску

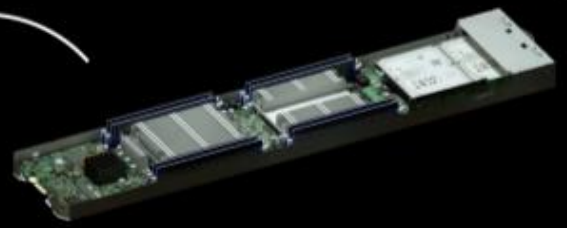
How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



❸ The compromised motherboards were built into servers assembled by Supermicro.



❹ The sabotaged servers made their way inside data centers operated by dozens of companies.

❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

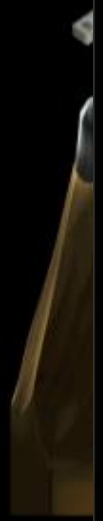
Illustrator: Scott Gelber

Bloomberg

How the Hack

. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.



❹ The sabotaged servers made their way inside data centers operated by dozens of companies.

Bloomberg Businessweek

October 8, 2018

The Big Hack

How China used a tiny chip to infiltrate America's top companies

❸ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.

❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

https://www.bloomberg.com/news/feature -america-s-top-companies

Illustrator: Scott Gelber

Bloomberg

TS]

Charter
of Trust

Charter of Trust

on Cybersecurity

И это прописная истина

Мы не можем ожидать от людей активной поддержки цифровой трансформации без **ДОВЕРИЯ** к безопасности данных и сетей.

Charter of Trust

Мы подписались за кибербезопасность!

Мы подписали Хартию Доверия.

enel IBM Munich Security Conference msc Münchner Sicherheitskonferenz NXP SIEMENS AES AIRBUS Allianz

Atos cisco DAIMLER DELL Technologies SGS T TOTAL TÜV SÜD

И мы пришли к 10 принципам

01 **Владение кибер и IT безопасностью**

02 **Ответственность через цифровой канал поставки**

03 **Безопасность по умолчанию**

04 **Ориентация на пользователя**

05 **Инновации и совместное созидание**

Charter of Trust

For a secure digital world

06 **Образование**

07 **Сертификация для критичных инфраструктур и решений**

08 **Прозрачность и ответственность**

09 **Регулятивные рамки**

10 **Совместные инициативы**

НМ 2018 - https://www.youtube.com/watch?v=Onx10FTZmlM

НМ 2019 - https://www.youtube.com/watch?v=Onx10FTZmlM см. с 7:03:23

Charter of Trust

Промышленная безопасность

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

SIEMENS
Ingenuity for life

Заинтересованные стороны по IEC 62443

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

https://bit.ly/2EHExH9 раздел по кибер безопасности

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)

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

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

CP

CP343-1 Advanced

CP443-1 & Advanced

CP1243-1

CP1543-1

CP1628

Распределенные

ET 200 PN/DP ЦПУ

ET 200SP PN ЦПУ

Сертифицированные брандмауэры

SCALANCE S

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

Активное сетевое оборудование

- Разработаны в соответствии с TIA концепцией
- Соотвествие SIMATIC System Requirements Specification Environment.
- Соответсвие NAMUR NE
- Соответствие Ж.Д. стандартам

siemens.com/switches-for-pa

SCALANCE SC-600

- Промышленные стандарты резервирования сетей
- Высокая производительность
- Высокая надежность и безопасность данных

siemens.com/scalance-s

SCALANCE W

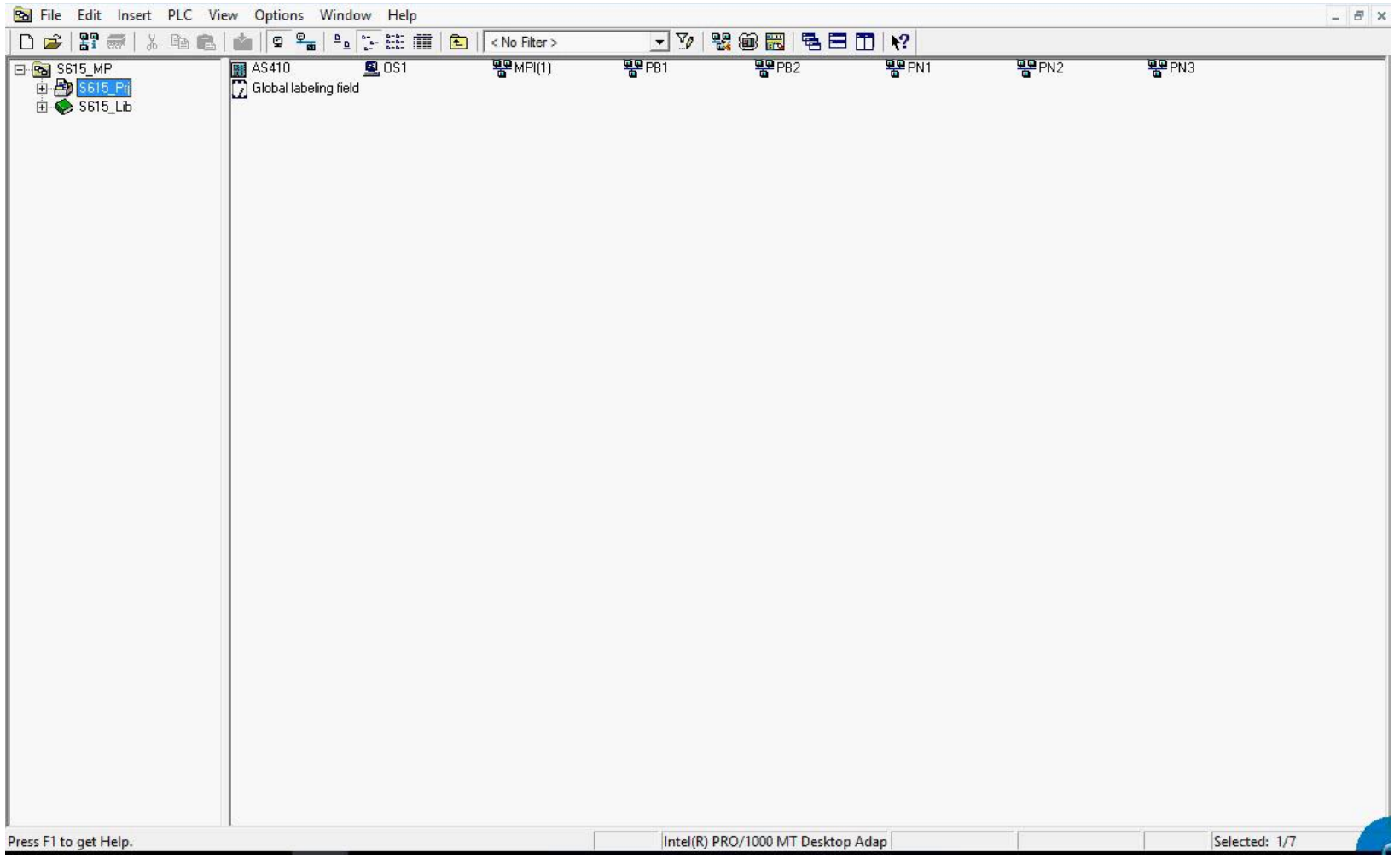
- Промышленные беспроводные коммуникации
- Надежность и безопасность
- Промышленные стандарты резервирования сетей

Пример :

siemens.com/scalance-w1748

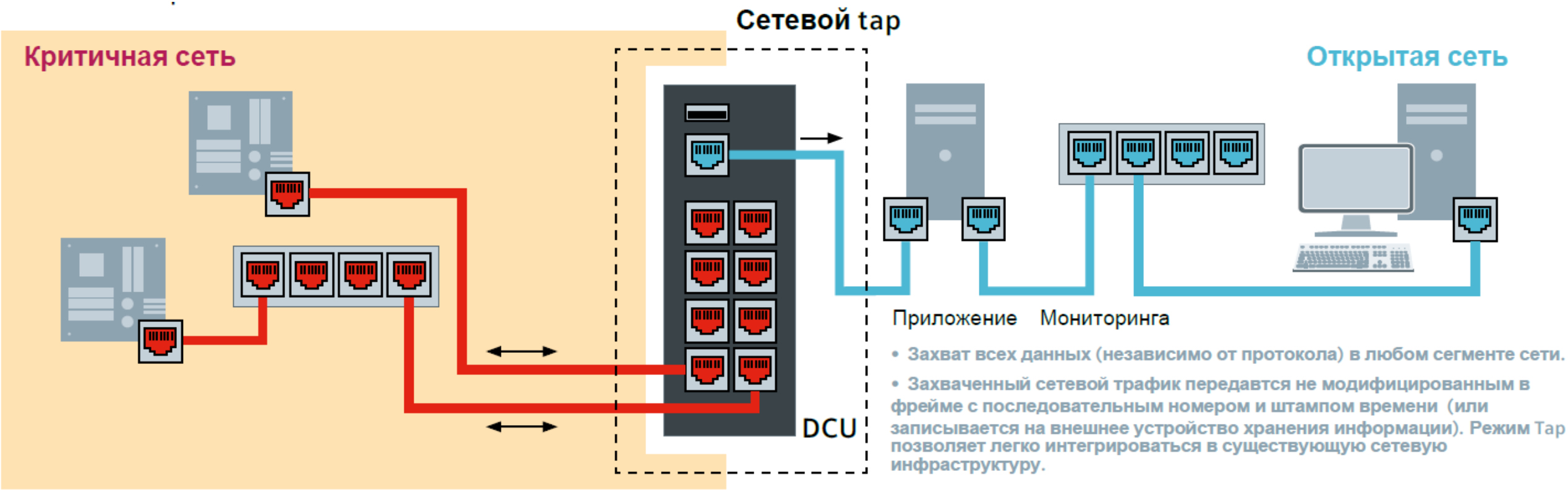
Интегрированное решение

- Интегрированная среда разработки АСУ ТП
  - Сети и узлы
  - Топология и подключения
  - Резервирование
  - VPN
  - Безопасный NTP
  - SNMP v3
  - Проч.
- Интеграция диагностики и топологии



DCU – Data capture unit
Модуль захвата данных – режим Tap

SIEMENS
Ingenuity for life

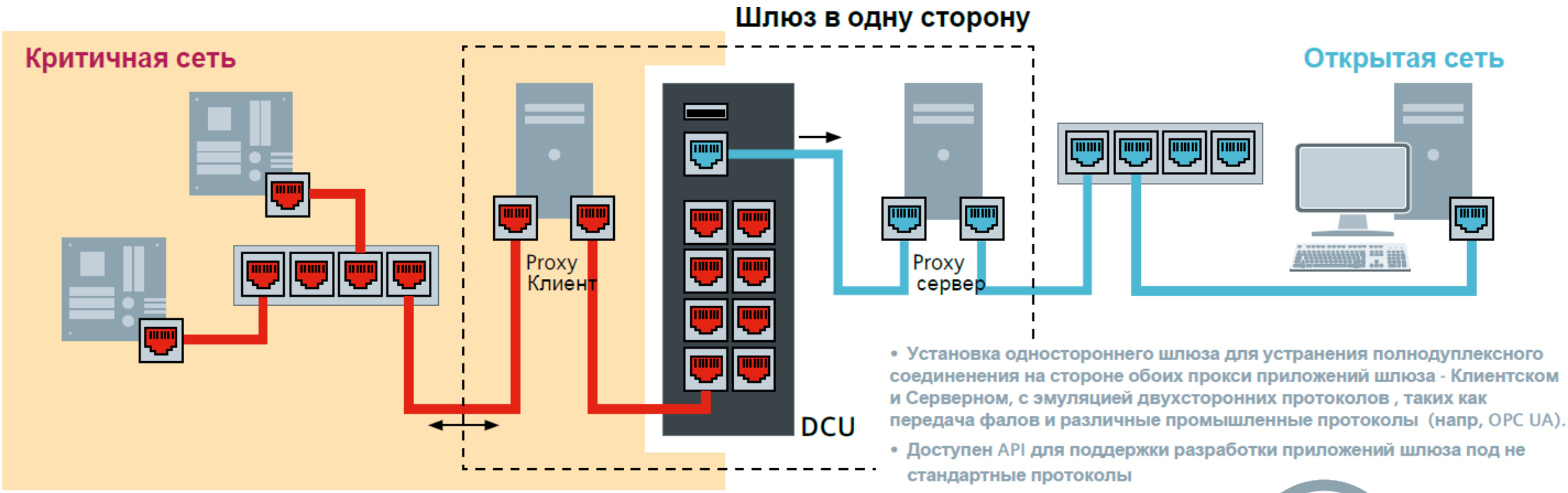


- Захват всех данных (независимо от протокола) в любом сегменте сети.
- Захваченный сетевой трафик передавтся не модифицированным в фрейме с последовательным номером и штампом времени (или записывается на внешнее устройство хранения информации). Режим Tap позволяет легко интегрироваться в существующую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

Также см. SCALANCE TAP104 https://support.industry.siemens.com/cs/ww/en/ps/6GK5104-0BA00-1SA2

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

https://siemens.com/dcu

Serhii Stepaniuk [RC-UA DI PR&TS]

Промышленная безопасность

Механическое закрытие неиспользуемых портов замком IE RJ45

IE RJ45 Port Lock

Возможности / функции		Преимущества
Механический замок для неиспользуемых интерфейсов RJ45 сетевого оборудования и устройств	▶	**Физическая безопансость** открытых, несипользуемых **RJ45 интерфейсов** для предотвращения неавторизованного доступа
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
Считыватель карт: Контроль доступа с SIMATIC RF1060R

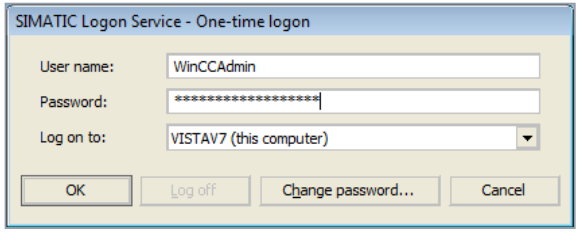
SIMATIC RF1060R

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

SIMATIC Logon

SIEMENS
Ingenuity for life



Требования клиента

- Централизованное управление пользователями
- Поддержка требований Food and Drug Administration (FDA)
- Конфигурирование «на лету»
- Интеграция системы безопасности с MS Windows
- Поддержка доменов и рабочих групп

Наше решение

Защищенный доступ с помощью SIMATIC Logon

Управление пользователями WinCC с помощью SIMATIC Logon…

- Централизованное администрирование (включая срок жизни пароля, auto logoff после неактивности, блокировка пользователя после введенного несколько раз неверно пароля, блокировка экрана)
- Конфигурирование «на лету» (добавить/ удалить / заблокировать учетные записи пользователей)
- Поддерживаются все конфигурации WinCC, включая web
- Поддерживается доменная концепции и рабочие группы Windows

Управление пользователями повысит безопасность Вашей системы

https://support.industry.siemens.com/cs/ww/en/ps/6ES7658-7BX61-0YA0

Serhii Stepaniuk [RC-UA DI PR&TS]

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

https://support.industry.siemens.com/cs/ww/en/ps/6GK1704-1VW05-0AA0

Промышленная безопасность
Управление удаленными метями: SINEMA Remote Connect

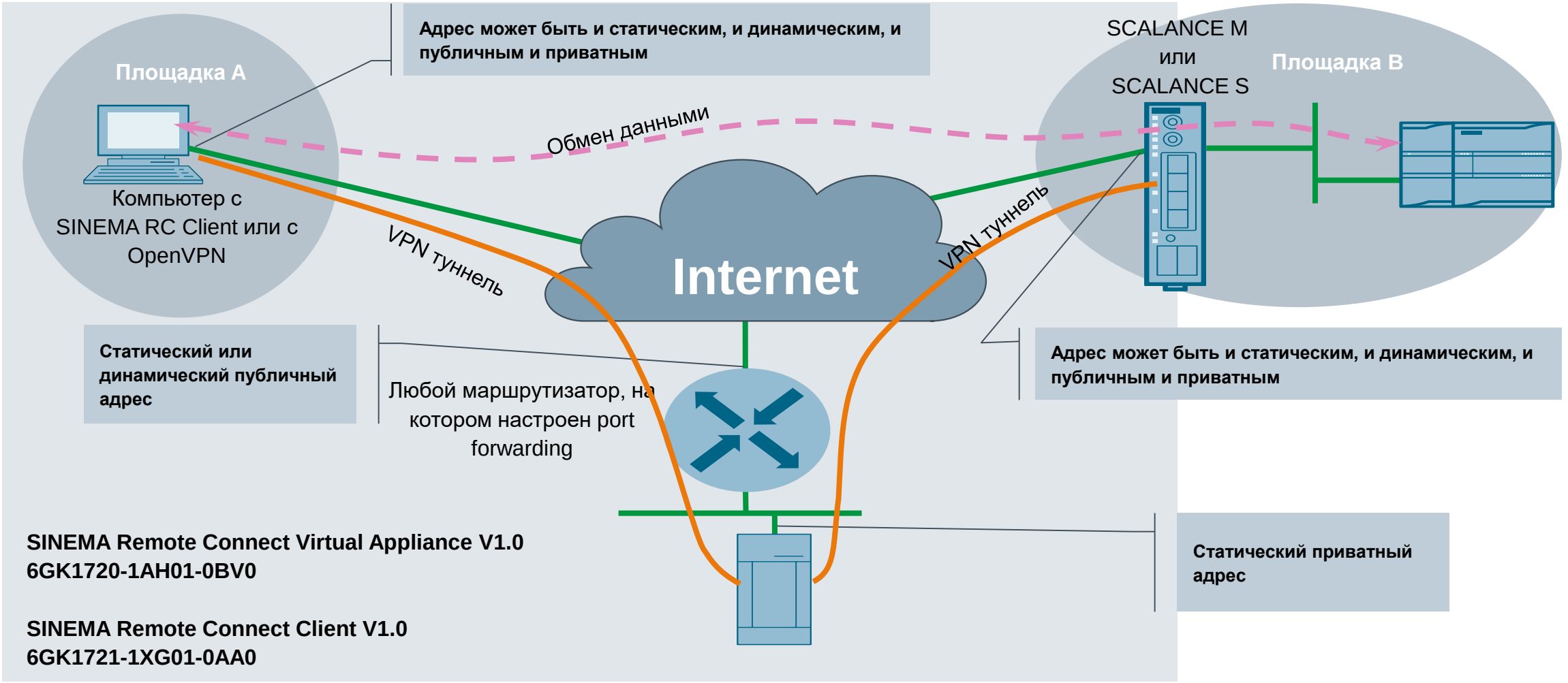
SINEMA Remote Connect

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.

https://support.industry.siemens.com/cs/ww/en/ps/6GK1721-1XG01-0AA0

Готовые решения удаленного доступа
SINEMA Remote Connect

SIEMENS
Ingenuity for life



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

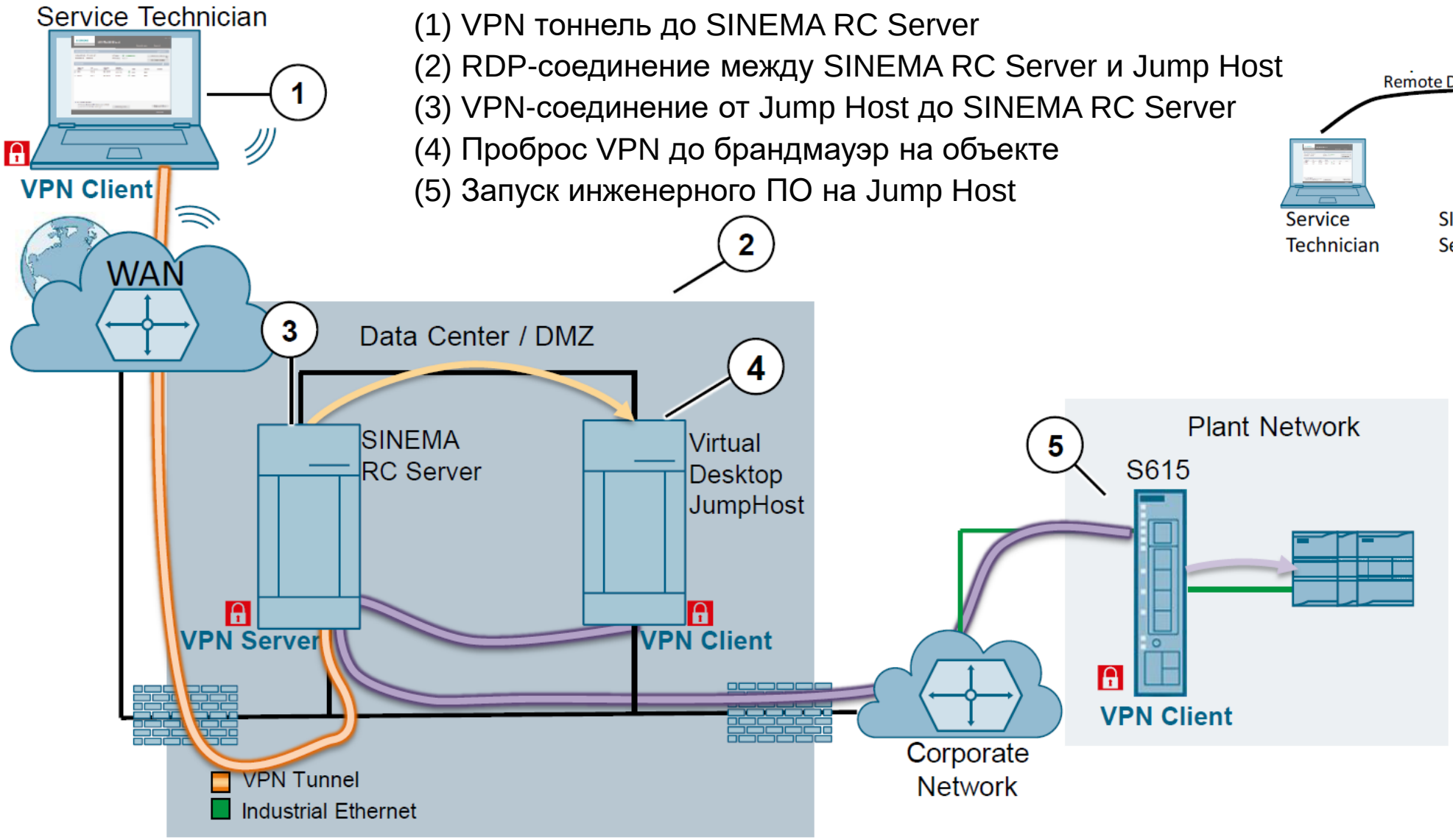
SINEMA Remote Connect Client V1.0
6GK1721-1XG01-0AA0

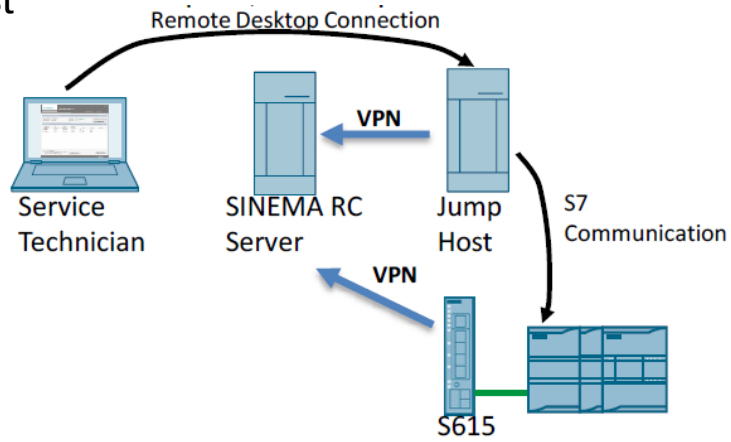
https://bit.ly/2EHExH9 раздел по кибер безопасности

Готовые решения удаленного доступа
SINEMA Remote Connect – Jump Host Application

SIEMENS
Ingenuity for life

(1) VPN тоннель до SINEMA RC Server
(2) RDP-соединение между SINEMA RC Server и Jump Host
(3) VPN-соединение от Jump Host до SINEMA RC Server
(4) Проброс VPN до брандмауэр на объекте
(5) Запуск инженерного ПО на Jump Host





Антивирусы и whitelisting

SIEMENS
Ingenuity for life

Требования клиента

Определение и блокирование вирусов, червей и троянских программ

Защита от:

- Нежелательного и вредоносного ПО
- Манипуляций

Наше решение

Внедрение **Антивирусов и белых списков (whitelisting)** позволяет осуществить следующие функции безопасности:

- Защита от вирусов, червей, троянских программ
- Предотвращение установки и работы нежелательных программ и вредоносного ПО
- Проверка ПО Siemens на совместимость с распространенным антивирусным ПО

Проверка ПО Siemens на совместимость с антивирусами: www.siemens.com/kompatool

Построение белых списков приложений
Информация по совместимости

SIEMENS
Ingenuity for life

Тестированная совместимость с McAfee Application Control

TIA Portal (status of: 30 Sep. 2017)
STEP 7 Basic V12
STEP 7 Basic V13
STEP 7 Professional V12
STEP 7 Professional V13
WinCC Advanced V12
WinCC Advanced V13
WinCC Basic V12
WinCC Basic V13
WinCC Comfort V12
WinCC Comfort V13
WinCC Professional V12
WinCC Professional V13
WinCC RT Advanced V12
WinCC RT Advanced V13
WinCC RT Professional V12
WinCC RT Professional V13

PCS 7 (status of: 30 Sep. 2017)
PCS 7 V9.0 – V9.0 SP1
PCS 7 V8.2 – V8.2 SP1
PCS 7 V8.1 – V8.1 SP1
PCS 7 V8.0 – V8.0 SP2
PCS 7 V7.1 – V7.1 SP4
PCS 7 V7.0 – V7.0 SP3
PCS 7 V6.1 – V6.1 SP4

WinCC (status of: 30 Sep. 2017)
WinCC V7.4
WinCC V7.3 SE Upd1
WinCC V7.3
WinCC V7.2
WinCC V7.0 – V7.0 SP3
WinCC V6.2 + SP3

SINUMERIK 840D (status of: 14. Sep. 2018)		MAC V5.1	MAC V6.2	MAC V7.0	MAC V8.1
IPC 427E Windows 10 LTSB	SINUMERIK Operate 4.8 SP2	x	x	--	✓
IPC 427D Windows 7 SP1	SINUMERIK Operate 4.5 SP2 bis 4.8 SP2	x	--	✓	x
PCU 50.5 Windows 7 SP1	HMI PRO sl 4.5 SP3 HF12	x	--	✓	x
	SINUMERIK Operate 4.5 SP2 bis 4.8 SP2	x	✓	✓	x
PCU 50.5 Windows XP SP3	SINUMERIK Operate 2.7 SP4 bis 4.8 SP1	x	✓	x	x
PCU 50.3 Windows XP SP2+	SINUMERIK Operate 2.6 SP1 bis 4.5 SP1	x	✓	x	x
	HMI Advanced 06.04.33 bis 7.6 SP2	x	✓	x	x
PCU 50.2 Windows XP SP1+	HMI Advanced 06.03.30 bis 06.04.33	x	✓	x	x
PCU 50.2 Windows NT4 SP6	HMI Advanced 06.03.30 bis 06.04.33	✓	x	x	x

✓ = compatible combinations -- = not tested combinations x = not compatible combinations

Больше информации : https://support.industry.siemens.com/cs/document/109750783

Обновленная информация по совместимости TIA Portal, PCS 7 / WinCC и других продуктов автоматизации Siemens : https://www.siemens.com/kompatool

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

SIEMENS
Ingenuity for life

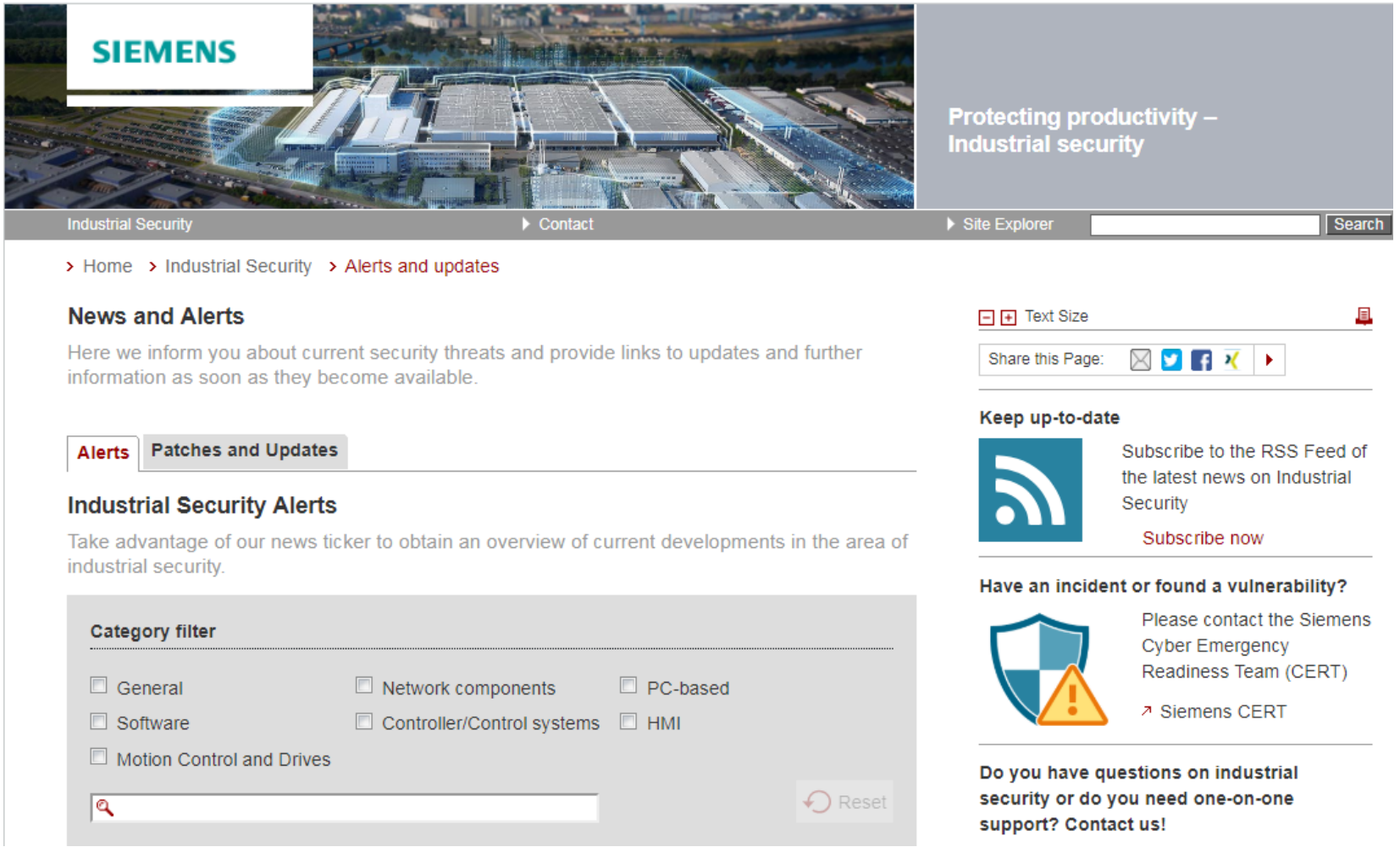
	A	B	C	D	E	F	G	H	I
1	PatchedProduct	PatchIdentifier1	PatchIdentifier2	ReleaseDate (YYYY-MM-DD)	Description	Patch Status	ReferenceInfo	PassedProduct	FailedProduct
2	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4338380)	KB4338380		2018-08-14	A security issue has been identified 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

Serhii Stepaniuk [RC-UA DI PR&TS]

Какие обновления необходимы для продуктов SIEMENS ?
Предупреждения промышленной безопасности

SIEMENS
Ingenuity for life

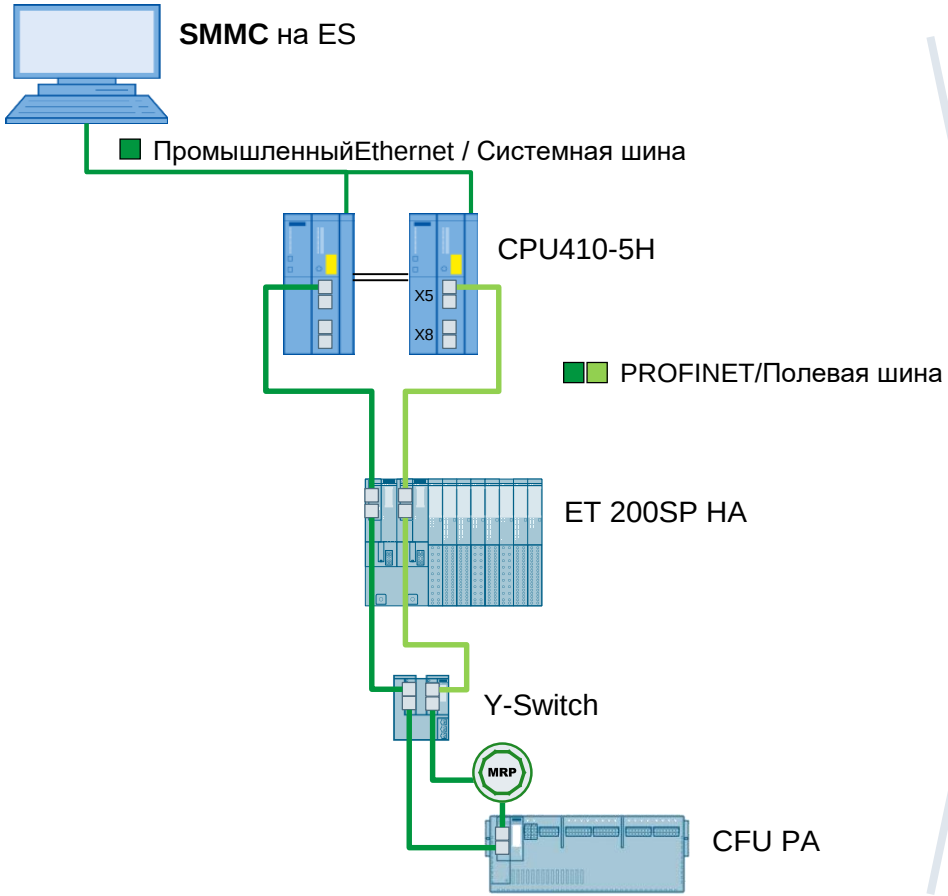


https://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/overview.aspx

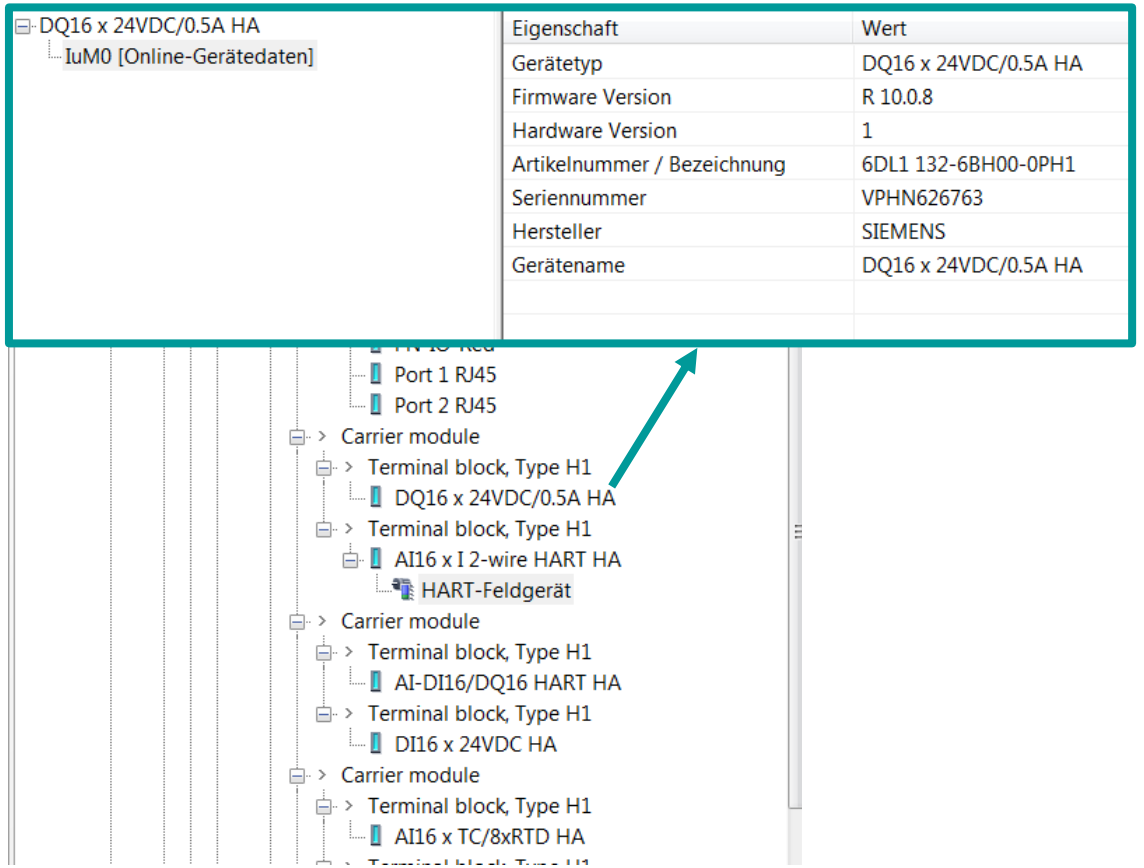
SIMATIC ET 200SP HA
I&M0 данные через SIMATIC Management Console (SMMC)

SIEMENS
Ingenuity for life

Установка

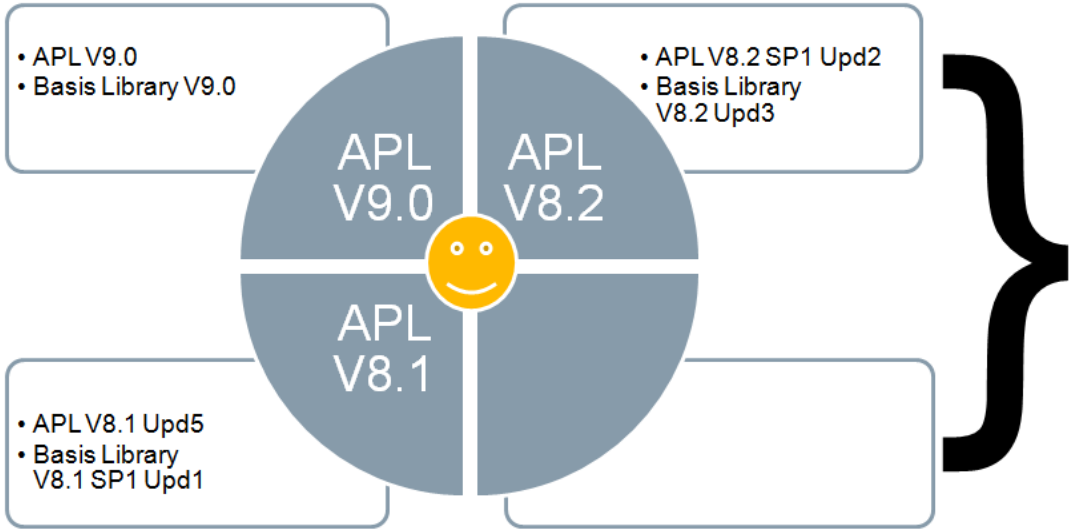


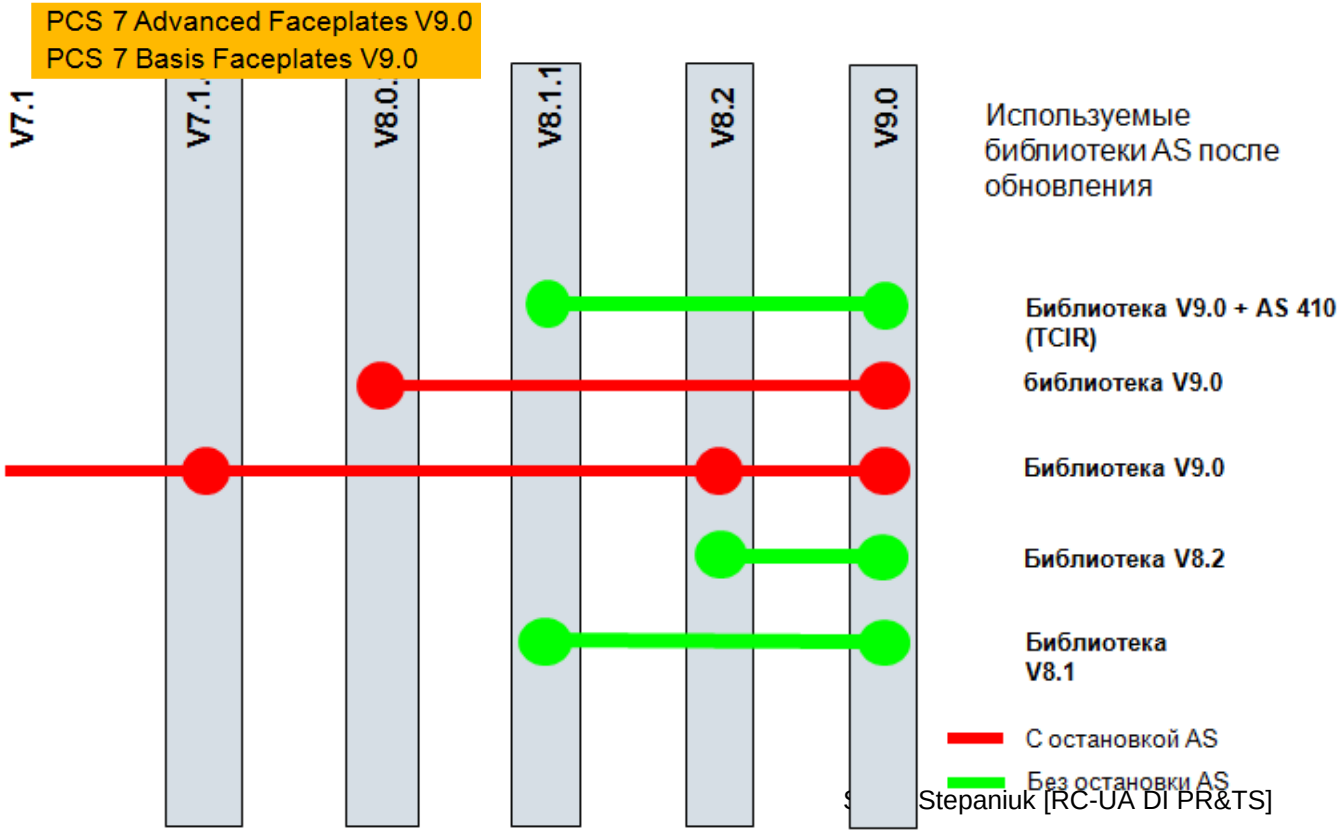
Как это выглядит на станции разработки



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

SIEMENS
Ingenuity for life



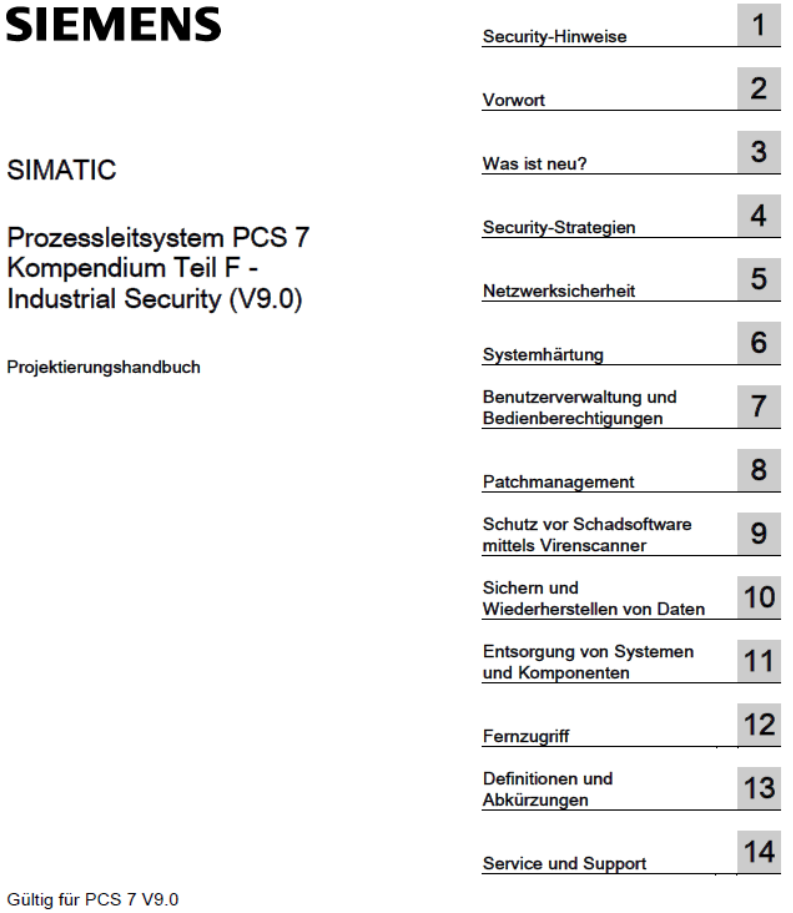


Концепция безопасности АСУ ТП PCS 7 CompendiumPart F

SIEMENS
Ingenuity for life

Руководство по построению информационной безопасности АС УТП PCS 7 в Compendium Part F

- Безопасность сети
- Усиление системы
- Администрирование авторизации пользователей и операторов
- Управление обновлениями
- Защита от malware с помощью антивирусных сканеров
- Резервное копирование и восстановление данных
- Удаленный доступ


SIEMENS

SIMATIC

Prozessleitsystem PCS 7
Kompendium Teil F -
Industrial Security (V9.0)

Projektierungshandbuch

Gültig für PCS 7 V9.0

03/2018
A5E43229005-AA

https://support.industry.siemens.com/cs/ww/de/view/109756871

Промышленная безопасность
Сертификация систем SIMATIC PCS 7

SIEMENS
Ingenuity for life


ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE
No. Z2 16 10 67801 001

Holder of Certificate: Siemens AG
PD PA AE
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
GERMANY

Production Facility(ies): 67801

Certification Mark:

Product: Industrial Control Systems and Components

Model(s): SIMATIC PCS 7

Parameters: Process Control System

Tested according to: PPP 50156B:2016
(based on IEC 62443-4-1)
IEC 62443-3-3(ed.1)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SK90104C

Valid until: 2019-10-20

Date, 2016-10-21 (Christian Dirmeier)

Page 1 of 1

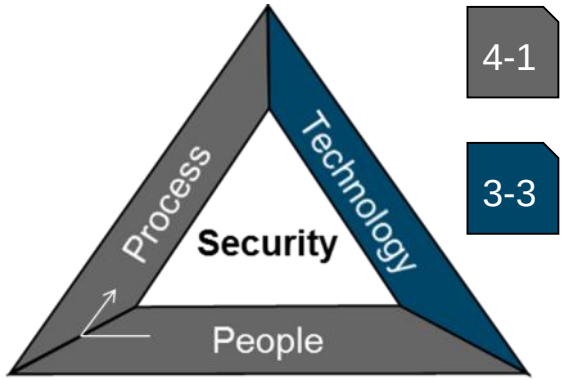
04052767560019

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

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 РСУ 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**

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

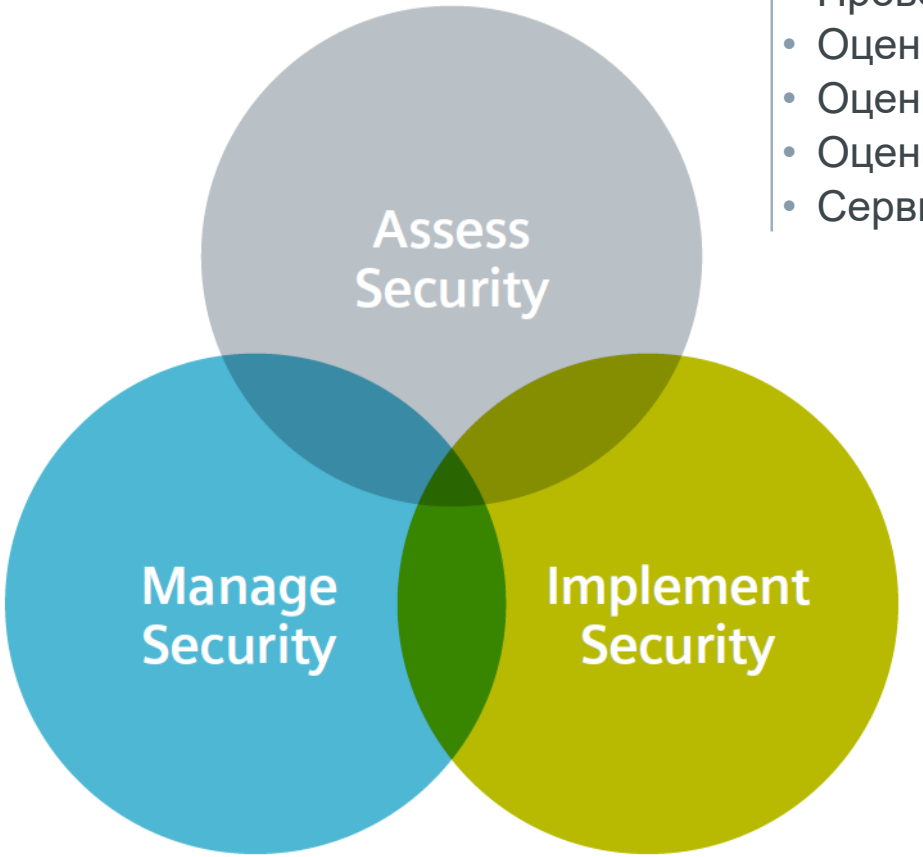
Целостность системы
- Усиление системы
- Управление исправлениями
- Обнаружение атак
- Аутентификация и защита доступа

Industrial Security Services
Портфолио решения киберзащиты

SIEMENS
Ingenuity for life

Assess Security

- Проверка промышленной безопасности
- Оценка IEC 62443
- Оценка ISO 27001
- Оценка рисков и уязвимостей
- Сервисы сканирования



Manage Security

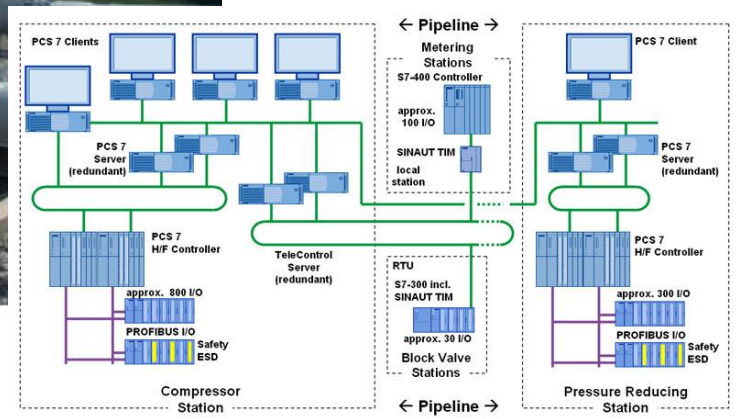
- Мониторинг промышленной безопасности
- Менеджер уязвимостей промышленной системы
- Управление обновлениями
- Удаленная обработка инцидентов

Implement Security

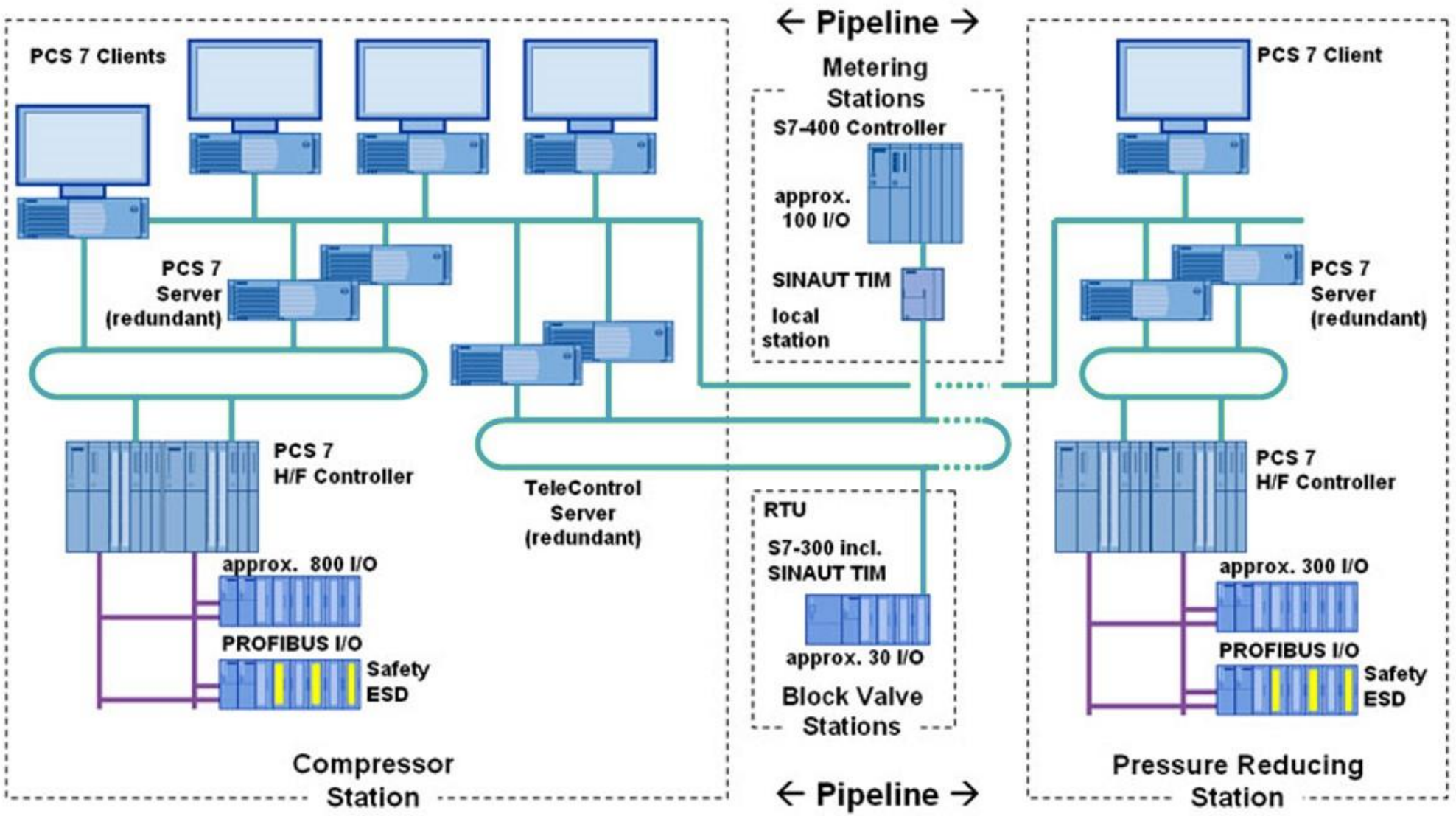
- Обучения по безопасности
- Консультации по промышленной безопасности
- Automation Firewall
- Белые списки приложений
- Антивирусы
- Детектирование аномалий в автоматике
- Решение мониторинга промышленной безопасности

Кибербезопасность в реальном мире – компрессорная станция

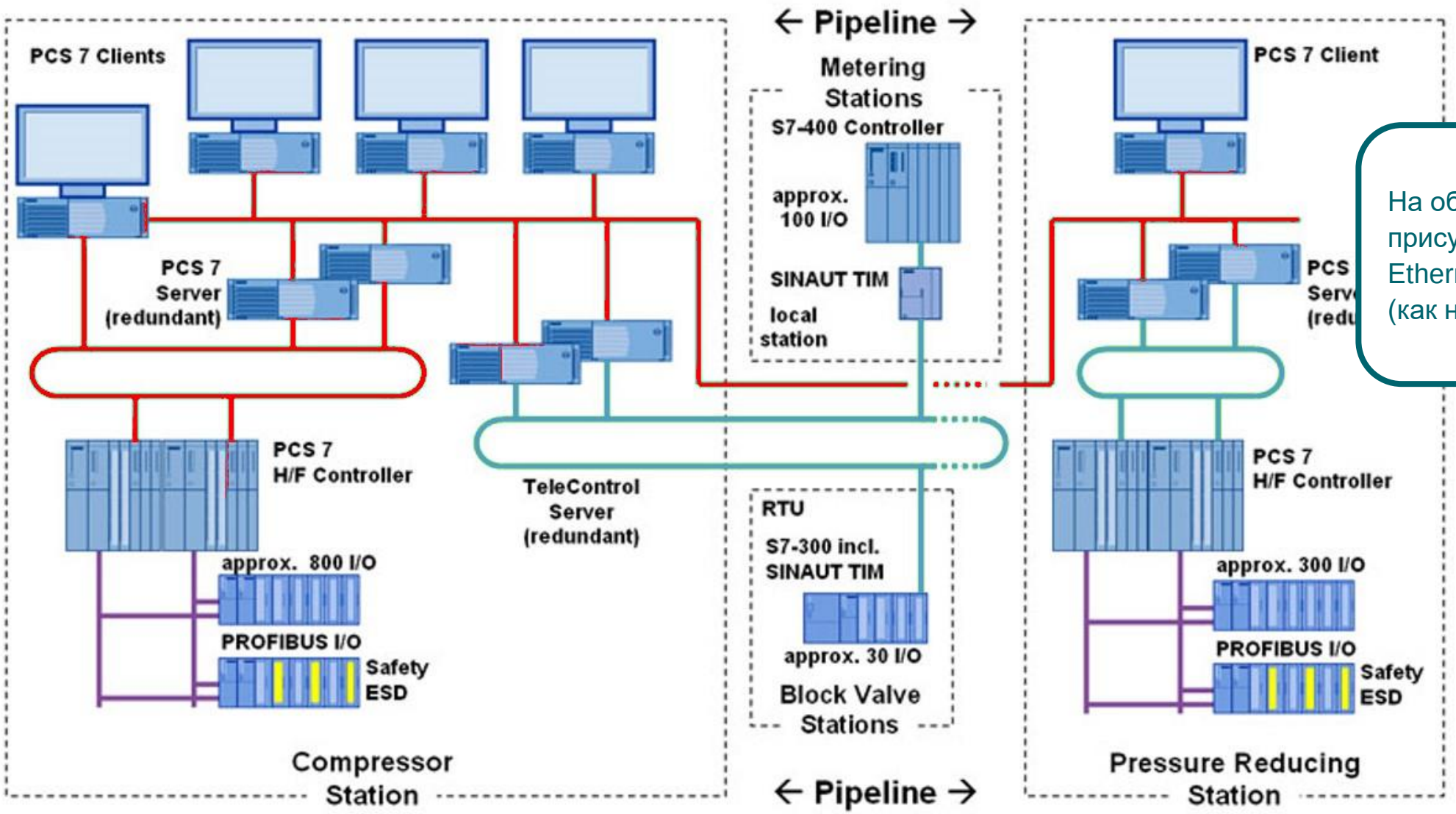
SIEMENS
Ingenuity for life



Типовая архитектура АСУ ТП

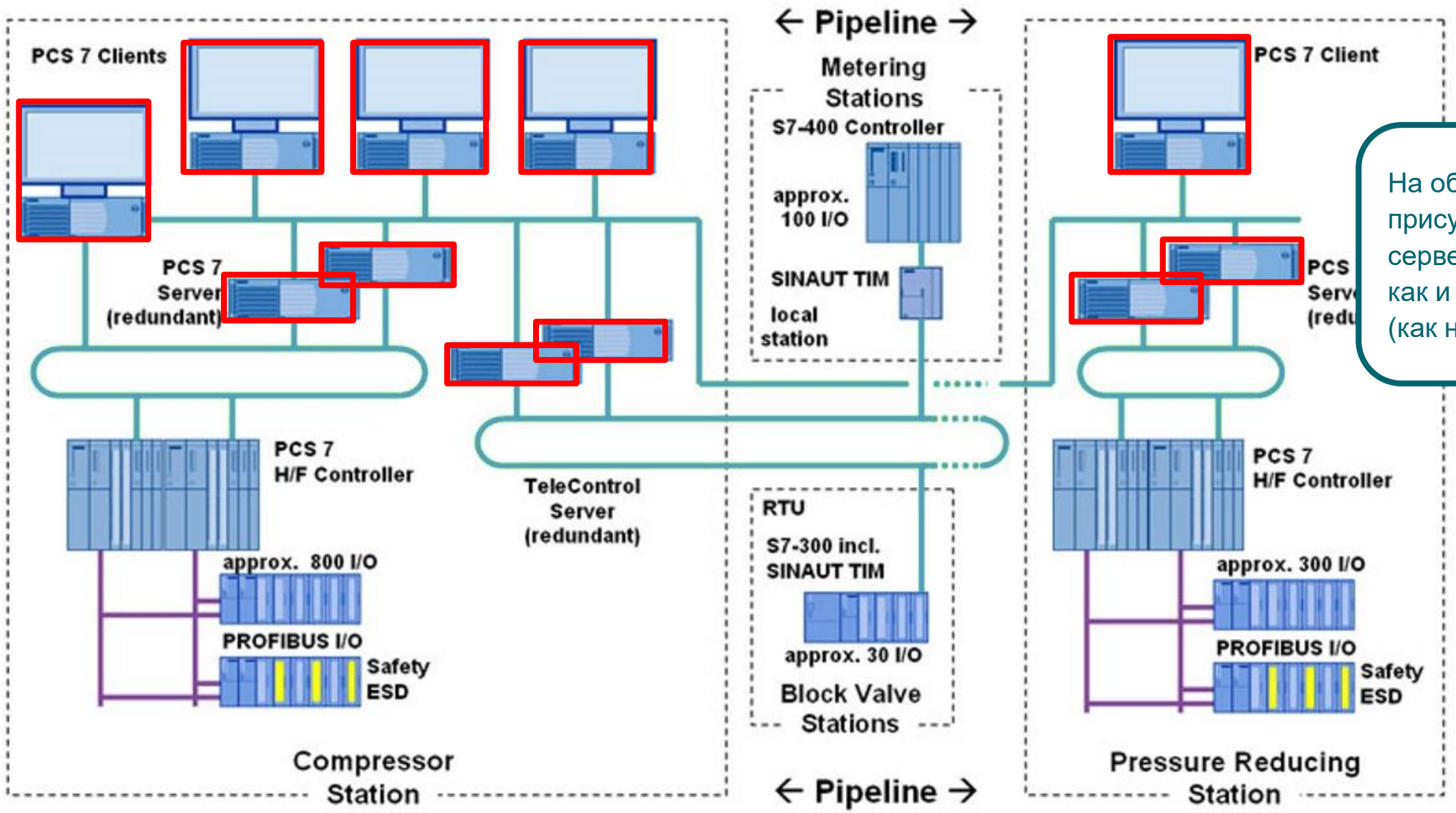


Типовая архитектура АСУ ТП



На объекте автоматизации присутствуют такие же Ethernet сети как и в офисе (как на уровне IT)

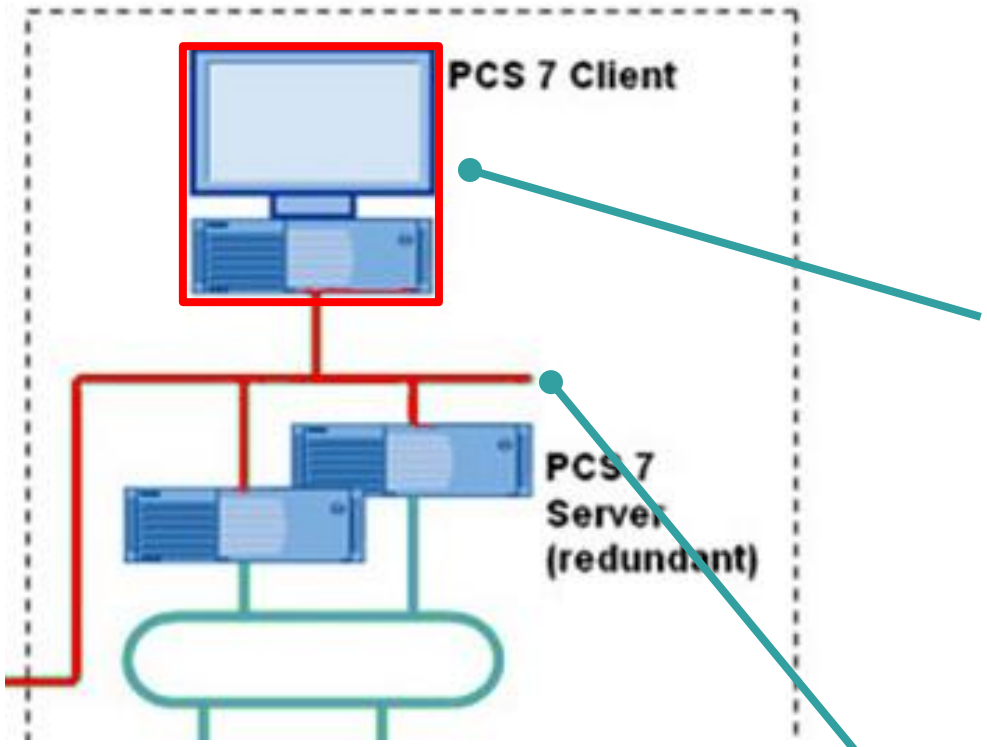
Типовая архитектура АСУ ТП



На объекте автоматизации присутствуют такие же сервера и рабочие станции как и в офисе
(как на уровне IT)

Применимы ли те же самые принципы кибербезопаснсоти на уровне OT как и на уровне IT ?

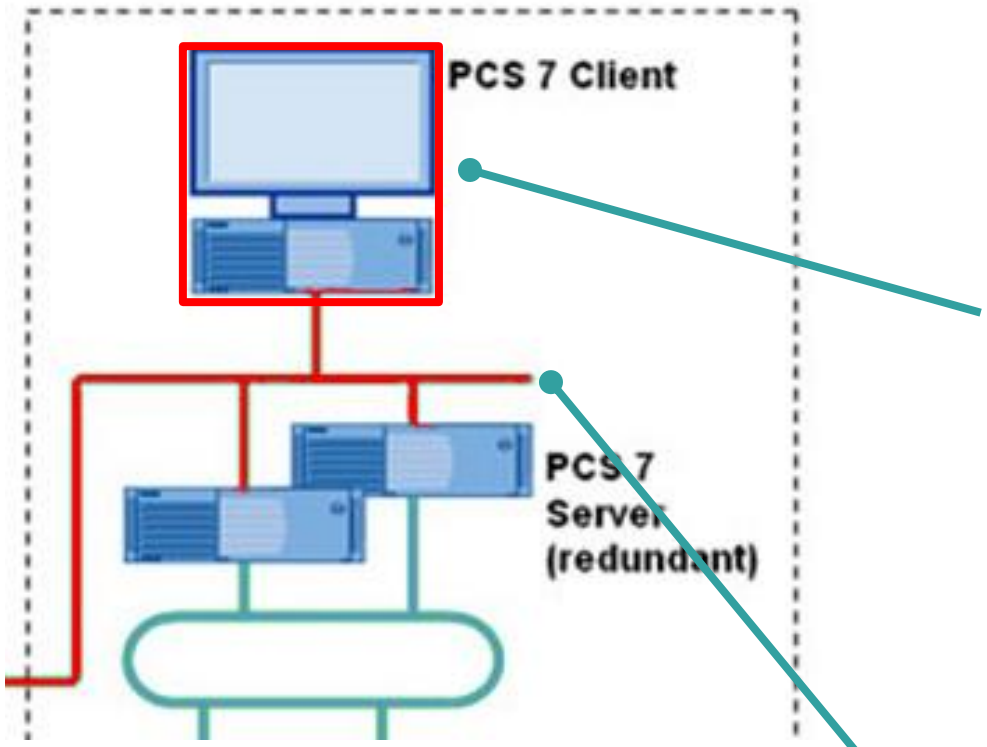
Типичные методы атаки



- Атакующий эксплуатирует уязвимость в ОС и другом используемом ПО.
  - Ошибки в ПО
  - Неиспользуемые сервисы Windows
  - Небезопасные, устаревшие коммуникационные протоколы системы
  - Слабые или общие пароли пользователей
  - Учетные записи по умолчанию
- Атакующий устанавливает вредоносное ПО для перехвата управления или блокировки ПК пользователя.
- Атакующий уничтожает или шифрует данные.
- ПК пользователей сети инфицированы и предоставляют доступ к сети АСУ ТП и ее ПК.
- Компьютеры мошенников подключены к сети АСУ ТП или соседним сетям для получения доступа в дальнейшем.

Что можно сделать для снижения риска атаки?

SIEMENS
Ingenuity for life



- ~~Атакующий эксплуатирует уязвимость в ОС и другом используемом ПО.~~
  - ~~Ошибки в ПО~~
  - ~~Неиспользуемые сервисы Windows~~
  - ~~Небезопасные, устаревшие коммуникационные протоколы системы~~
  - ~~Слабые или общие пароли пользователей~~
  - ~~Учетные записи по умолчанию~~

- ~~Атакующий устанавливает вредоносное ПО для перехвата управления или блокировки ПК пользователя.~~
- ~~Атакующий уничтожает или шифрует данные.~~

- ~~ПК пользователей сети инфицированы и предоставляют доступ к сети АСУ ТП и ее ПК.~~

- ~~Компьютеры мошенников подключены к сети АСУ ТП или соседним сетям для получения доступа в дальнейшем.~~

Снижение рисков

Управление обновлениями ПО

“Усиление” системы и мониторинг уязвимостей

Защита от Malware и "белые списки" приложений

Аварийное резервное копирование и восстановление

Брандмауэры следующего поколения

“Белые списки” компьютеров

Что где устанавливается ?

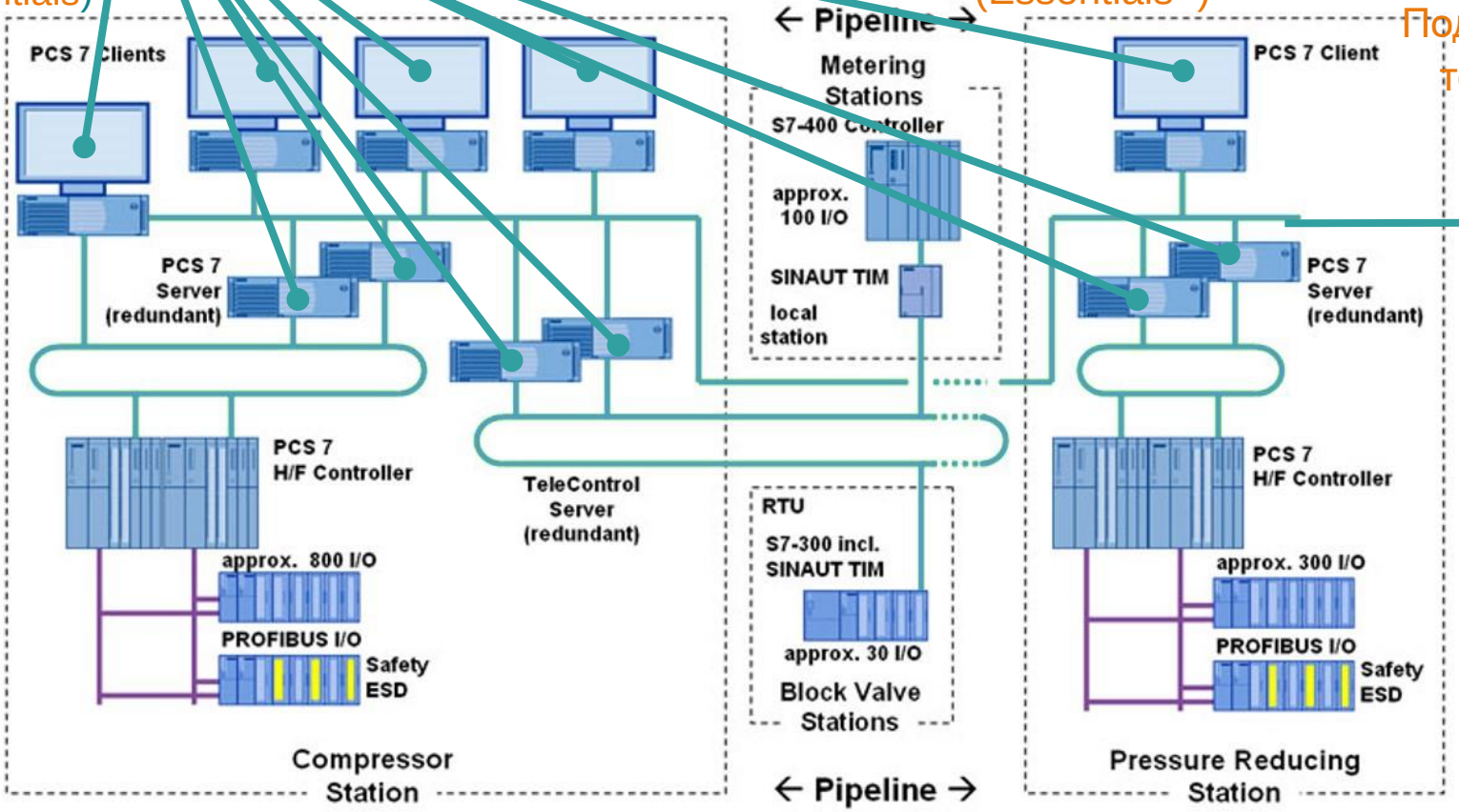
SIEMENS
Ingenuity for life

Обновления ПО,
Белые списки,
Усиление систем (Basic);
Агенты защиты от malware (Essentials)

Сервер непрерывного мониторинга уязвимостей (Essentials+)

Подключение только на чтение

Брандмауэр следующего поколения (Коммуникации)



Подключенные к сети хранилища для резервных копий, Промышленные ПК Siemens Серверов мониторинга и управления (Essentials)

System Hardening (Укрепление системы)

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Устройства и узлы часто сконфигурированы с конфигурациями по умолчанию, которые зачастую не безопасны • «Не укрепленные» узлы - основной вектор атаки • Требуется соответствие лучшим практикам и политикам безопасности заказчика • Антивирус не часть стандартной сборки	• Общие ошибки в конфигурации или не оптимальная настройка безопасности по умолчанию • IT отдел сфокусирован на задачи эксплуатации вместо безопасности	• Конфигурация узлов и других систем с использованием “стандартов усиления безопасности” (конфигурация системных брандмауэров, антивирусов, фильтрации MAC адресов, белых списков приложений, проч.)	• Общие ошибки в конфигурации невозможно эксплуатировать • Снижение площади атаки (ограничивая доступные и открытые службы и порты) • Существенно повышена общая безопасность среды • Соответствие NERC, NIST, ISO, IEC, ISA….

Пример укрепления:

- Разрешены требования к сложности пароля (где доступно)
- Разрешен мониторинг портов
- Разрешена фильтрация MAC на использованных физических портах (Scalance)
- Разрешены задачи сценариев укрепления
- Есть проверка входов в систему
- Запрещены не критичные для ОС учетные записи пользователей

- Настройка **Входа в систему и сетевого** (опционально)
- **Усиление правил брандмауэра** и списков управления доступом (опционально)
- Активация функции **Белых списков приложений** (опционально)
- Оценка систем **безопасного резервного копирования и восстановления** systems and procedures (опционально)
- **Обновления безопасности и приложений Anti-Malware** (опционально)
- Применение **системных политик безопасности и процедур** (опционально)
- **Запрещение не использованных портов** и сервисов (Физическое и виртуальное) (опционально)
- **Шифрование** требуемых коммуникационных портов (опционально)
- **Ужесточение паролей** для всех систем где технически выполнимо (опционально)

Whitelisting (Белые списки)

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Традиционные антивирусы не предоставляют защиту от атак 0-дня и полиморфных вирусов • Плохая видимость и контроль над работающими приложениями • Рост кибер атак берущих начало в узле • Незащищенные узлы уязвимы для атак	• Сложность и большая зона атаки современных приложений и ОС • Отсутствие детального контроля над разрешениями на запуск для отдельных исполняемых файлов	• McAfee Integrity Control сконфигурирован Siemens для использования с ПК системы управления Контроль целостности обеспечивает, что только доверенные приложения разрешены к запуску на ПК. • Контроль целостности одобрен для различных программных продуктов Siemens	• Предотвращение выполнения неизвестных приложений и исполняемых файлов • Обеспечивается видимость и контроль над приложениями, независимо от используемых портов и протоколов • Тестированные и одобренные для использования с конкретными компьютераим АСУ снижает риск Bring-Your-Own-Device (BYOD) • Не требуется непрерывного обновления сигнатур или шаблонов • Допущение обновления ОС без выключения защиты

Patch Management (Управление обновлениями)

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Число выявленных уязвимостей выросло на 111% с 2013. • Число критичных уязвимостей выросло на 60% с 2013. • Обновления совершенно обязательны, независимо от размера компьютерных систем • Преимущества обновлений должны балансировать с требованиями доступности и эксплуатационной готовности	• Кибер угрозы динамичные и изощренные • Сложность современных приложений и ОС • Гибкие практики разработки	• Применение обновлений протестированных и одобренных Siemens для конкретных систем автоматики • Решение разработанное в комбинации know-how Безопасности и экспертизы в системах управления	• Обновления направлены на стабильность работы ОС и/или устранение уязвимостей. • Регулярная и своевременная установка обновлений является жизненно важным элементом всеобъемлющей концепции безопасности • Снижение вероятности ошибочного применения обновлений и как результат угрозы доступности предприятия • Обеспечивается соответствие требованиям

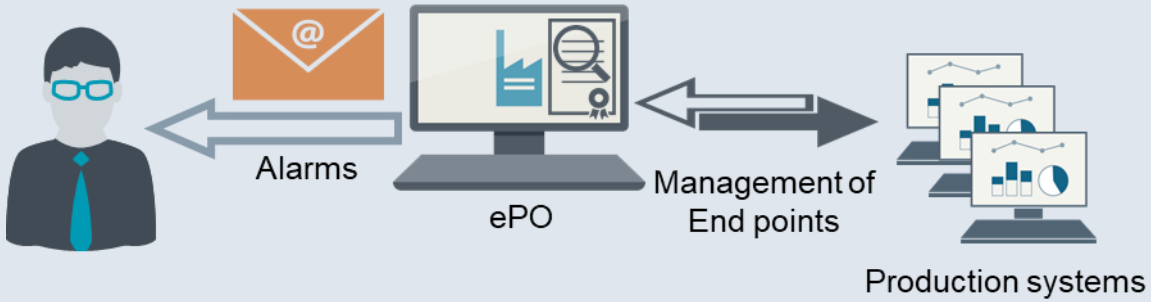
	A	B	C	D	E	F	G	H	I
1	PatchedProduct	PatchIdentifier1	PatchIdentifier2	ReleaseDate (YYYY-MM-DD)	Description	PatchStatus	ReferenceInfo	PassedProduct	FailedProduct
2	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4338380)	KB4338380		2018-08-14	A security issue has been identified 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**

Protection Management Server (Сервер менеджмента защиты)

SIEMENS
Ingenuity for life

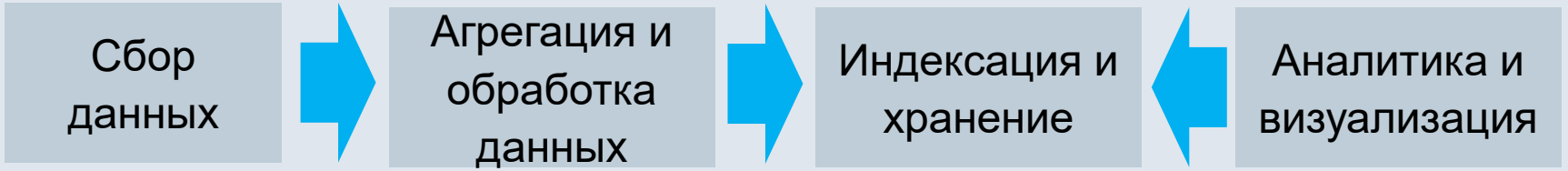
Проблема	Причина	Решение	Преимущества
• Неравномерное состояние ПО защиты узлов на разных ПК • Возможно инфицирование системы из-за устаревших патернов вирусов • Возможные угрозы malware из-за недостатка мониторинга антивирусного решения • Трудоемкий процесс выполнения изменений, например для новых систем	• Отсутствие общих платформ кибер безопасности • Не определены процедуры обработки событий управления безопасности	• Siemens предоставляет и конфигурирует McAfee ePO сервер для управления ПО защитой узлов • Пред-заданные наборы политик и правил для компонентов АСУ ТП • Встроены процедуры управления событиями безопасности	• Автоматизированное разворачивание и конфигурирование ПО защиты узлов • Централизованное управление обновлением ПО защиты • Информационные панели безопасности, отчеты и KPI



Log Server (Сервер журналов)

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Неавторизированные изменения в ПО и настройках • Необнаруженные атаки на компоненты АСУ ТП • Необнаруженные потери данных • Необнаруженные проблемы в приложениях	• Большое число разносторонних записей в журналах • Отсутствие коллектора нормализованных журналов с правилами классификации • Трудоемкий процесс рассмотрения журналов	• Siemens предоставляет и конфигурирует систему Security Event Management для обработки и хранения событий безопасности всех компонентов системы управления • Web интерфейс просмотра событий и визуализации • Пред-настроенный поиск	• Быстрая реакция на события безопасности • Лучше эффективность программы безопасности • Автоматическая фильтрация и аналитика событий • Хранение журналов безопасности • Пред-настроенные по конкретную систему информационные панели и отчеты



Аварийное восстановление: Резервное копирование и восстановление

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Возможность потери данных и программ из-за кибер атаки или физической катастрофы • Потенциальная потеря доступности оборудования, доверия заказчиков и репутации из-за длительного восстановления затронутых компонентов системы автоматики	• Отсутствие плана восстановления после аварии • Отсутствие решения для резервного копирования и восстановления • Плохо управляемый процесс резервного копирования	• Настроенное Siemens решение менеджмента резервного копирования и восстановления на базе лидера - ПО Acronis • Безопасное хранение и создание резервных копий • План восстановления после аварии обеспечивает быстрое восстановление после кибер инцидента	• План восстановления после аварии оптимизированный под конкретного заказчика и систему • Полное резервное копирование информации системы управления без влияния на производи-тельность системы • Упреждающая защита резервных фалов от ransomeware • Безопасное централизованное управление процессом резервного копирования и восстановления • Быстрое восстановление

Управление уязвимостями

SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Непрерывный поток обнаруженных новых уязвимостей • Изменение конфигурации и обновления представляют новые слабые стороны • Традиционное сканирование может повлиять на доступность компонентов системы автоматики	• Злоумышленники пытаются получить не санкциони-рованный доступ • Ошибки в коде ПО	• Программное решение управления уязвимостями установленное и сконфигурированное экспертами Siemens • Единый взгляд на уязвимости независимо от производителя • Ежегодная подписка на сервис Siemens • Passive and safe, OT-native Решение based on Nessus Network Monitor	• Освобождает ресурсы копаний, фокусируясь только на наиболее критические события, опираясь на экспертизу Siemens • Интеллектуальная работа с уязвимостями опирающаяся на аналитику для быстрой приоритезации и исправлений • Лучше понимание влияния кибер рисков на эксплуатацию и как с ними обходиться

Cyber Vulnerability Assessment (CVRA)
Оценки кибер-уязвимости

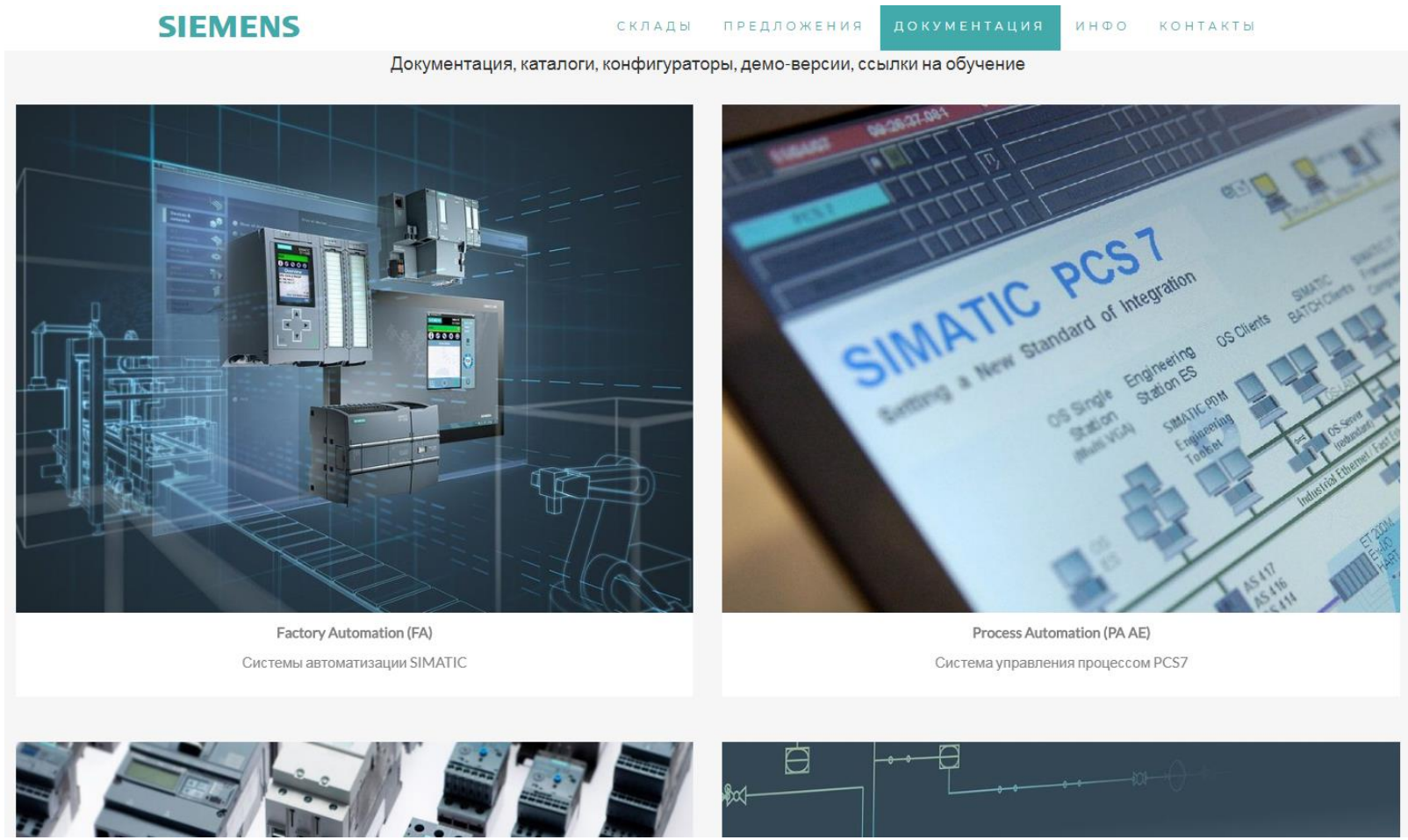
SIEMENS
Ingenuity for life

Проблема	Причина	Решение	Преимущества
• Постоянный поток обнаруженных новых уязвимостей • Изменения в конфигурации или развитие системы привносит новые слабые стороны	• Злоумышленники пытаются получить не санкциониро-ванный доступ • Ошибки в коде программ • Регуляторные требования • Разрывы в координации и осведомленности	• Сканирование уязвимостей для выявления потенциальных уязвимостей и угроз • Обновление систем • ОТ тестирование и усиление устройств	• Определение приоритетности обновлений на основе их критичности • Идентификация известных уязвимостей • Улучшенная безопасность по всей сети

Объем поставки:

- Основано на ISO 27002, NERC CIP, IEC 62443 -3-3 & -2-2
- Определение Параметров электронной безопасности (Electronic Security Parameter (ESP)) / Зон и каналов безопасности
- Определение всех портов и сервисов
- Определение слабых сторон безопасности в целевой с системе
- Сканирование всей сети и портов включая внутренние роутеры, брандмауэры и коммутаторы
- Обзор маршрутов и конфигураций каналов удаленного доступа.
- Ранжирование каждой выявленной уязвимости на Критичную, Высокую, Среднюю, и Низкую степень влияния
- Оценка управления доступом, конфигурация аккаунтов
- Идентификация уязвимостей или потенциальных угроз
- Детальная документация по Оценке кибер уязвимостей (Cyber Vulnerability Assessment (CVA) по результатам и оценённым система

Презентации по Кибербезопасности и полезные ссылки



https://www.siemens-products.online/

https://bit.ly/2EHExH9 раздел по киебр безопасности

SIMATIC PCS 7 V9.0
Спасибо за внимание!

SIEMENS
Ingenuity for life

Сергей Степанюк

PCS7 Leading specialist

100% foreign owned subsidiary Siemens Ukraine
RC-UA DI PR&TS
Ул. Ярославская 58
04071 Киев, Украина
Тел.: +380 44 392-2322
Моб.: +380 68 538-2322
E-Mail: serhii.stepaniuk@siemens.com

siemens.com/pcs7-v9

ГОРИЗОНТ УГРОЗ 2021

SIEMENS
Ingenuity for life

2019

- Преднамеренные перебои интернета ставят на колени торговлю
- Вымогатели похищают IoT
- Привилегированные инсайдеры принужденные к сотрудничеству
- Автоматическая дезинформация мгновенно завоевывает доверие
- Поддельная информация ставит под угрозу производительность
- Потеря доверия к скомпрометированными блок-чейнами
- Законы о надзоре раскрывают корпоративные секреты
- Правила конфиденциальности мешают отслеж. внутренних угроз
- Стремительное развертывание ИИ ведет к неожиданным результатам

2020

- Кибер и физические атаки комбинируют для расшатывания бизнеса
- Спутники приводят к хаосу на земле
- Вооруженные устройства обезоруживают организации
- Гонка квантовых вооружений подрывает цифровую экономику
- ИИ расширяет возможности злоумышленников
- Атаки на подключенные автомобили тормозят работу
- Биометрия дает ложное чувство безопасности
- Новые законы увеличивают риски и бремя соблюдения
- Надежные профессионалы разглашают слабые стороны организаций

2021

- 5G технологии расширили поверхность атак
- Манипуляция машинным обучением сеет замешательство
- Паразитическое ПО пирует на критической инфраструктуре
- Государственный шпионаж за технологиями нового поколения
- Саботированные облачные сервисы заморозили работу
- Дроны становятся хищниками и жертвами
- Цифровые общества военнизируют раскрытие уязвимостей
- Большие технологии разваливают бизнес модели

3.3 Поспешность в цифровой трансформации разрушает доверие

https://www.securityforum.org/research/threat-horizon-2021-the-digital-illusion-shatters/