Кибербезопасность последнего рубежа промышленной безопасности: систем противоаварийной защиты

Антон Шипулин
CISSP, CEH, CSSA

Менеджер по развитию решений
по безопасности критической инфраструктуры
Лаборатория Касперского

KASPERSKY

Система противоаварийной защиты (ПАЗ/SIS)

Приборная система безопасности (SIS)
Система контроля и управления, которая используется для выполнения одной или нескольких функций безопасности и состоит из одного или нескольких датчиков, из одного или нескольких логических устройств и из одного или нескольких исполнительных элементов.

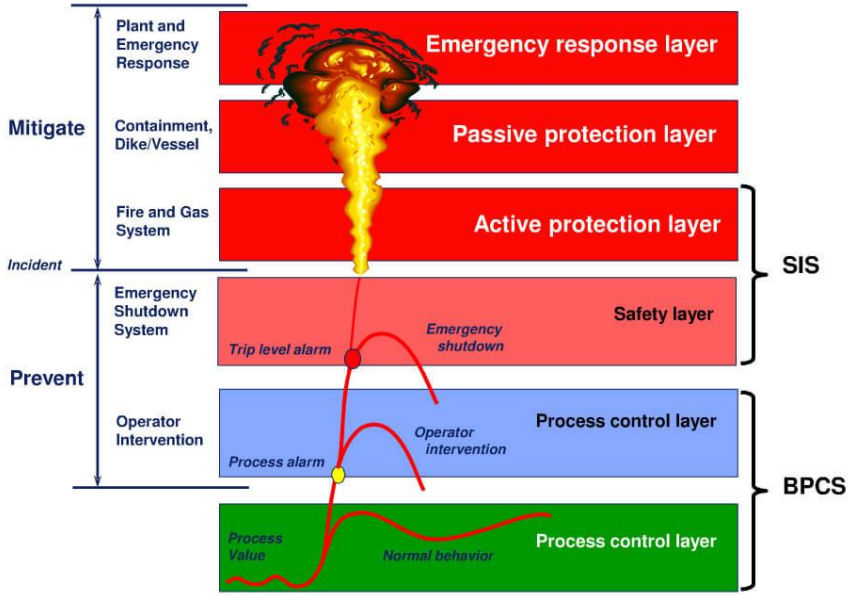
Источник: ГОСТ Р МЭК 61511-3-2011

Противоаварийная защита
Комплекс устройств, обеспечивающих защиту, предупреждение и (или) уменьшение опасных последствий аварийных ситуаций при эксплуатации систем инженерно-технического обеспечения и увеличение ресурса работы (срока службы) указанных систем.

Источник: 30.12.2009г. № 384-ФЗ

Противоаварийная защита
Системы и средства, обеспечивающие для взрывоопасных технологических процессов контроль параметров, определяющих взрывоопасность процесса, с регистрацией показаний и предаварийной (при необходимости - предупредительной) сигнализацией их значений, а также средствами автоматического регулирования и предаварийной защиты, включая безопасную остановку или перевод процесса в безопасное состояние по заданной программе.

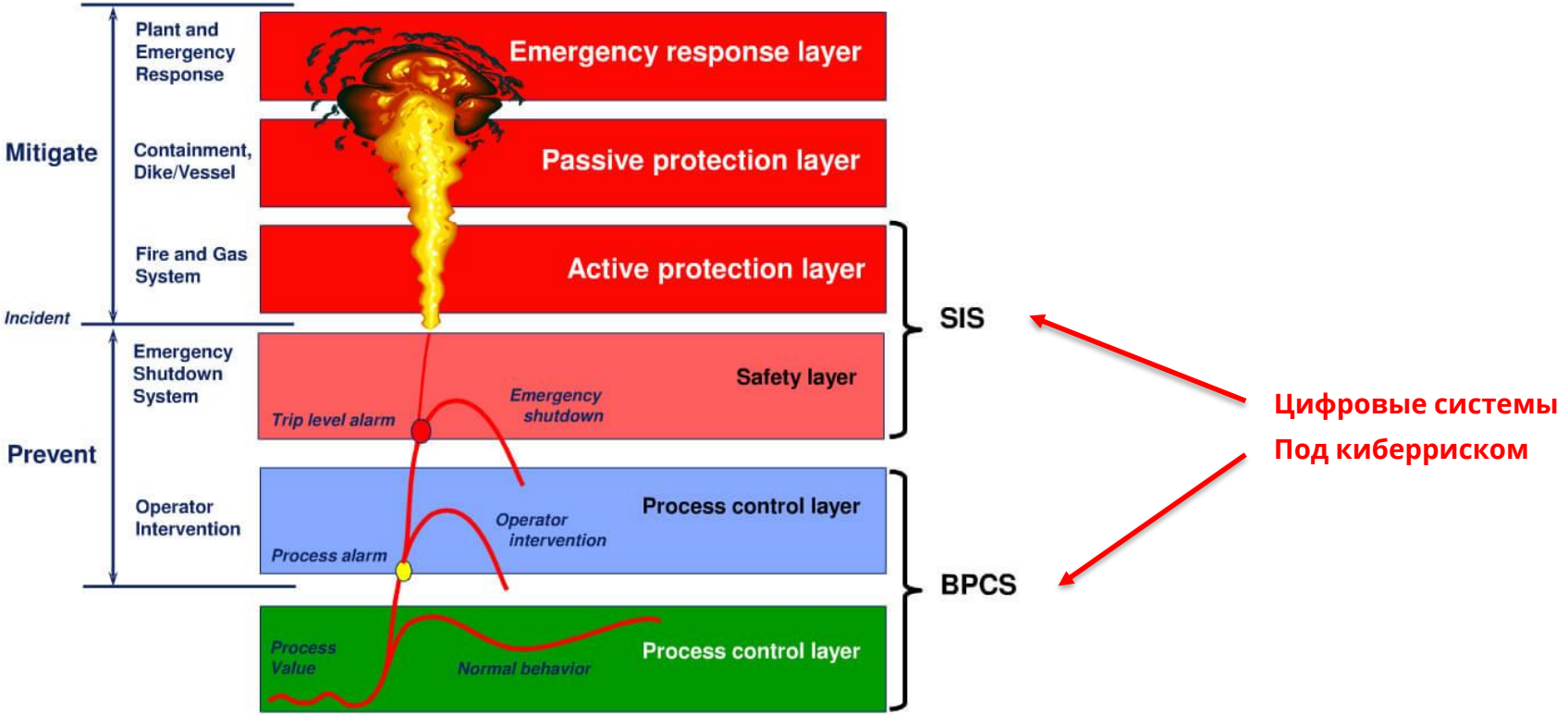
Источник: ПБ 09-540-03, ПБ 09-566-03.



Сближение систем управления и противоаварийной защиты

- Двустороннее сетевое взаимодействие или общая сеть
- Общие интерфейсы администрирования (инженерная станция)
- Общие репозитории хранения параметров и конфигураций
- Использование одинаковых учетных записей
- Использование общих полевых устройств (датчиков и активаторов)
- Объединение функцией на одном устройстве или платформе

Safety & Control convergence!



Цифровые системы
Под киберриском

DHS LOGIIC SIS Project 2010

Результаты исследования кибербезопасности ПАЗ

- Проблемы
- Рекомендации

Атаки на сетевые соединения:

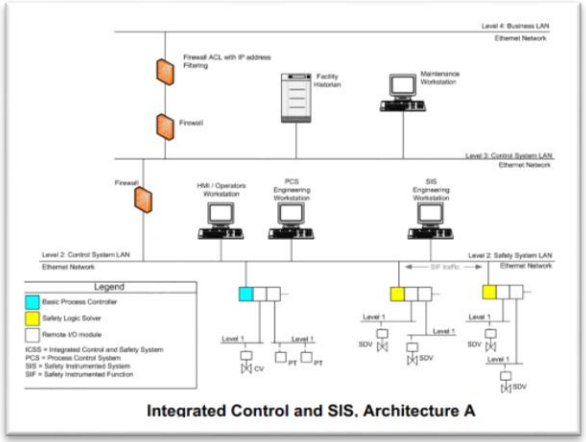
- ARP specific attacks (Grammar, Host Reply Storm, Cache Request Storms, Saturation, etc.)
- Ethernet specific attacks (Broadcast Storm, Fuzzer, Grammar, Multicast Storm, Unicast Storm, etc.)
- ICMP and IGMP specific attacks (Fuzzer, ICMP Storm, Type/Code Cross Product, V3 corruption)
- IP specific attacks
- TCP/UDP specific attacks

Методы атак

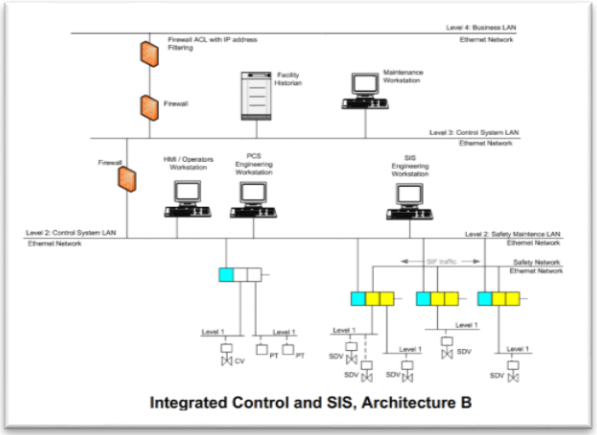
- modified network sniffing,
- traffic replay,
- data injection,
- signal interrupt messaging,
- bitflipping and integrity impact tests,
- payload injection attacks,
- resource starvation,
- cryptographic analysis,
- password cracking,
- privilege escalation,
- directory traversal,
- forced error manipulation,

Источник

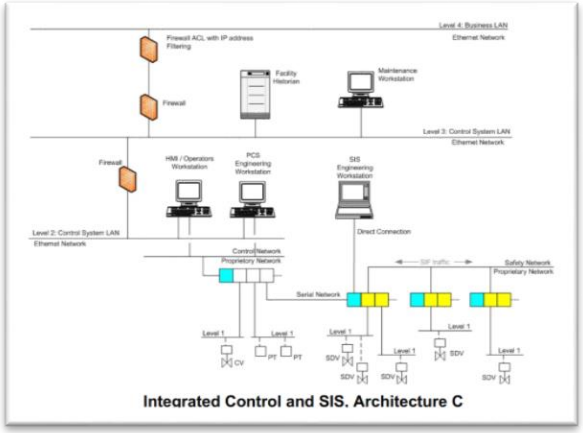
DHS LOGIIC SIS Project 2010 / Три типа архитектур



Integrated Control and SIS, Architecture A



Integrated Control and SIS, Architecture B



Integrated Control and SIS, Architecture C

Архитектура A

- Общая сеть АСУ ТП и ПАЗ
- Иногда общий АРМ инженера
- Общие базы данных

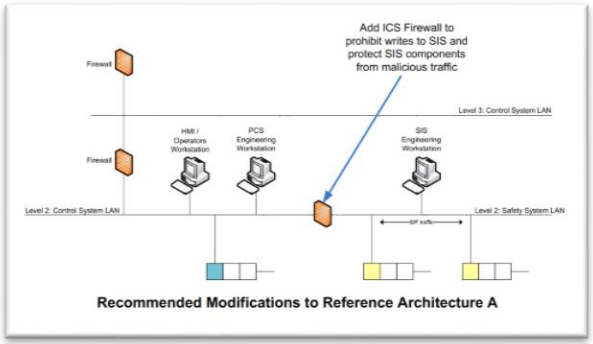
Архитектура B

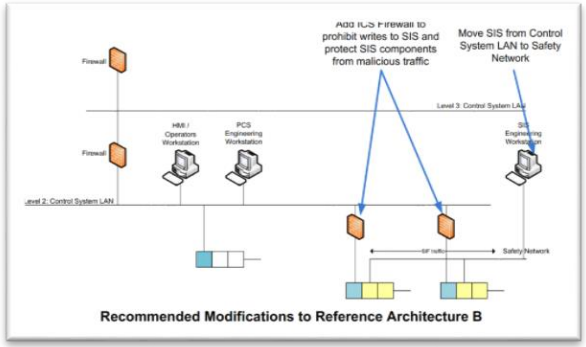
- Инженерный АРМ в общей сети
- Контроллеры ПАЗ в общей сети
- Выделенная сеть между ПАЗ

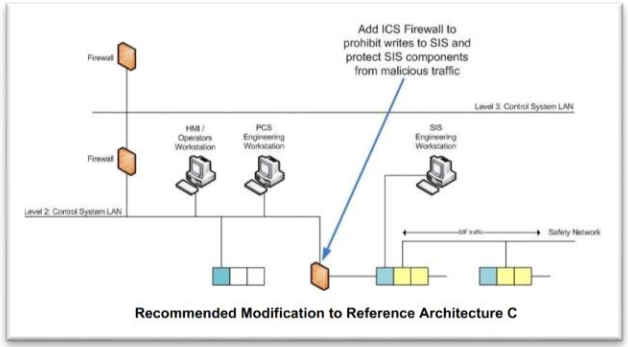
Архитектура C

- Инженерный АРМ подключен по последовательному интерфейсу к ПАЗ
- Контроллеры ПАЗ подключены в сети АСУ ТП через шлюз либо по последовательному интерфейсу
- Выделенная сеть между ПАЗ

DHS LOGIIC SIS Project 2010 / Архитектурные рекомендации







Архитектура A

- Использование МЭ
- Следование рекомендациям безопасности от производителей

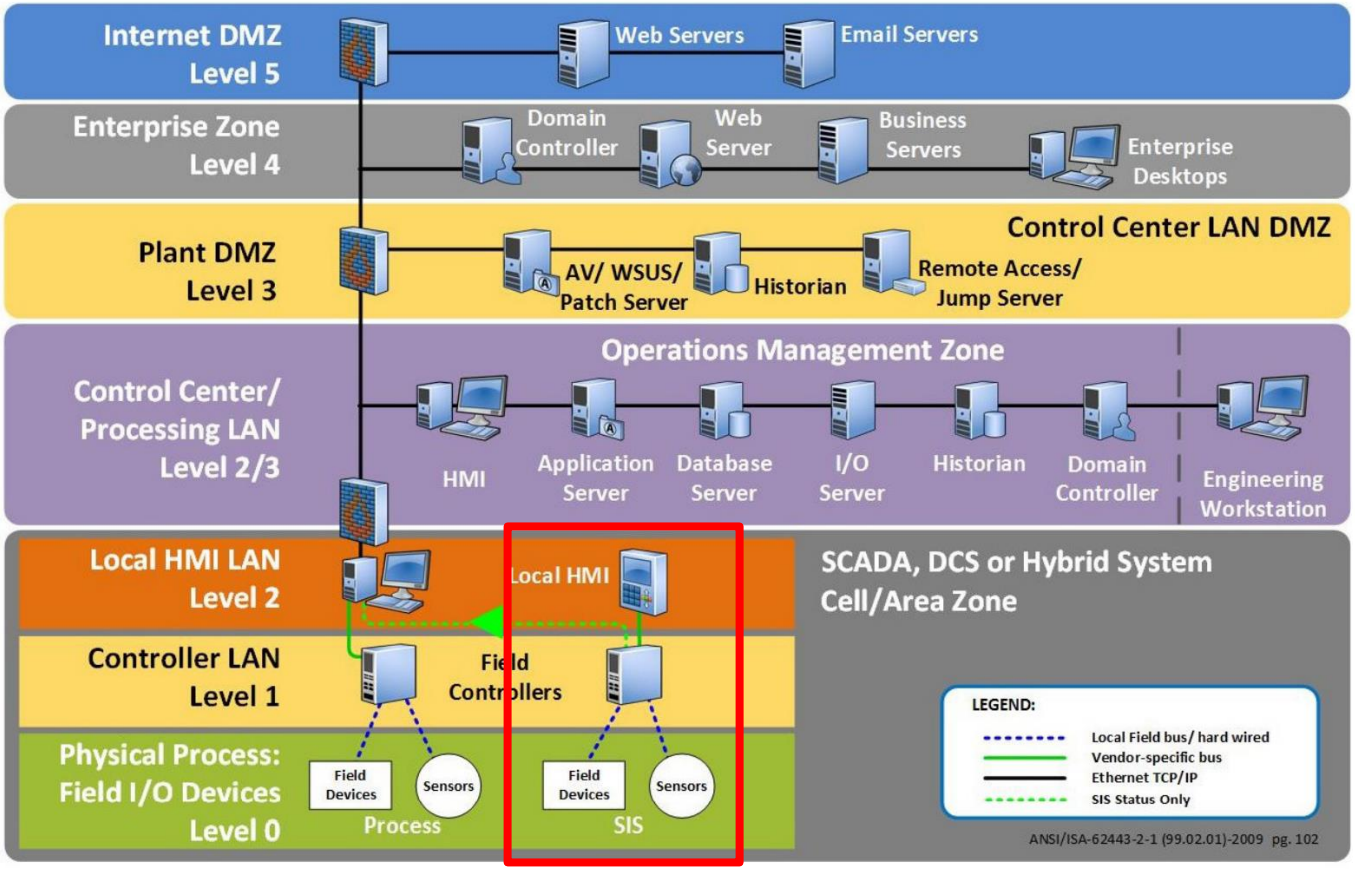
Архитектура B

- Использование МЭ
- Перенос инженерного АРМ в выделенную сеть
- Следование рекомендациям безопасности от производителей

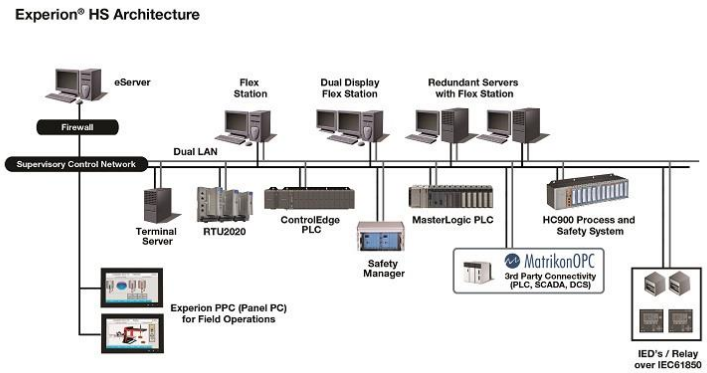
Архитектура A

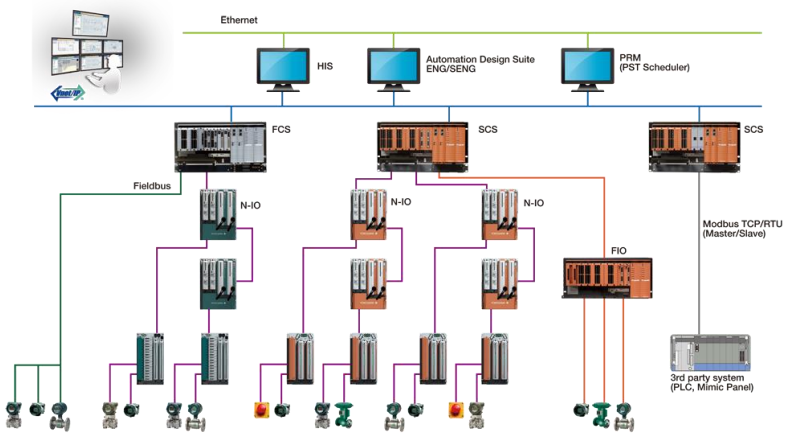
- Использование МЭ
- Следование рекомендациям безопасности от производителей

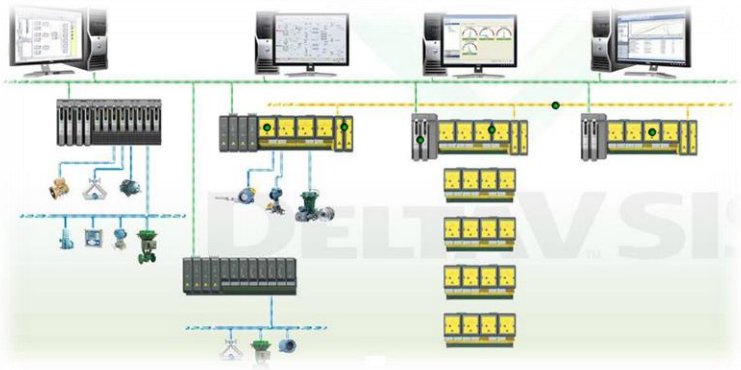
DHS / IEC 62443 Референсная архитектура



Примеры из жизни: общая сеть Honeywell / Yokogawa / Emerson



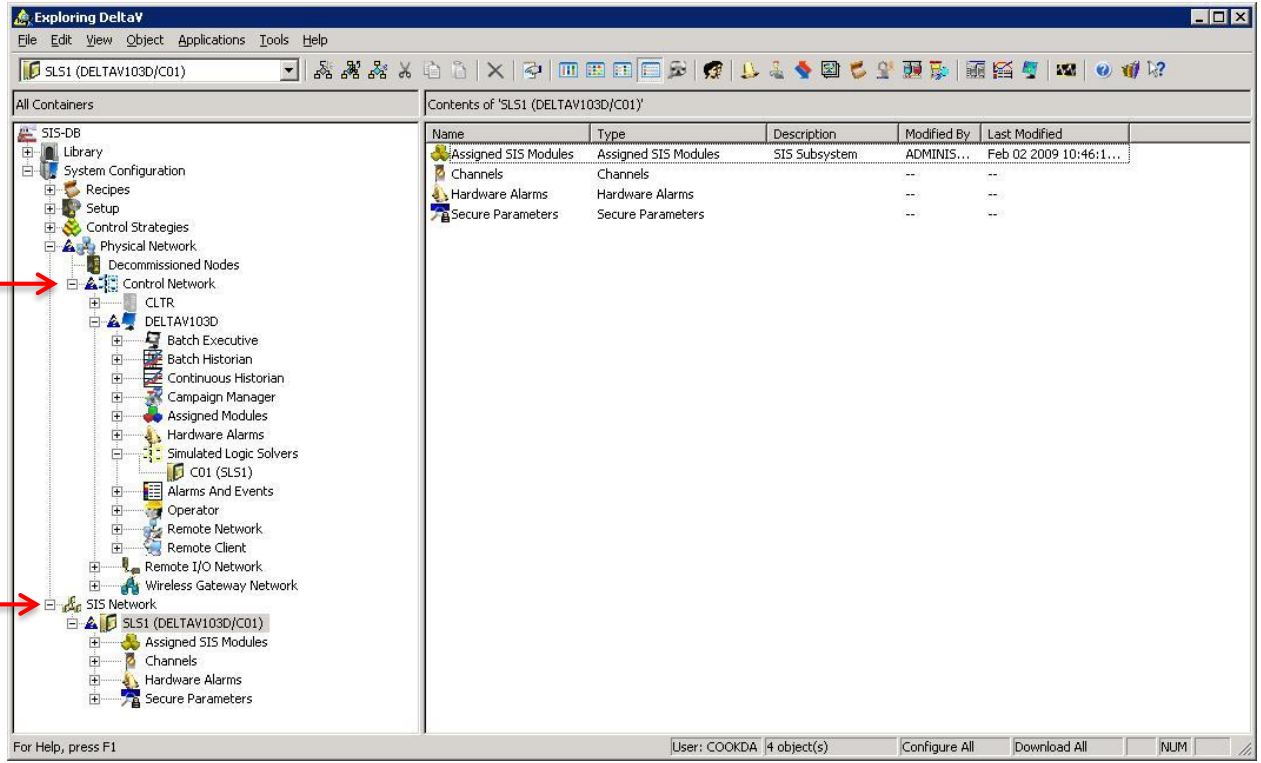




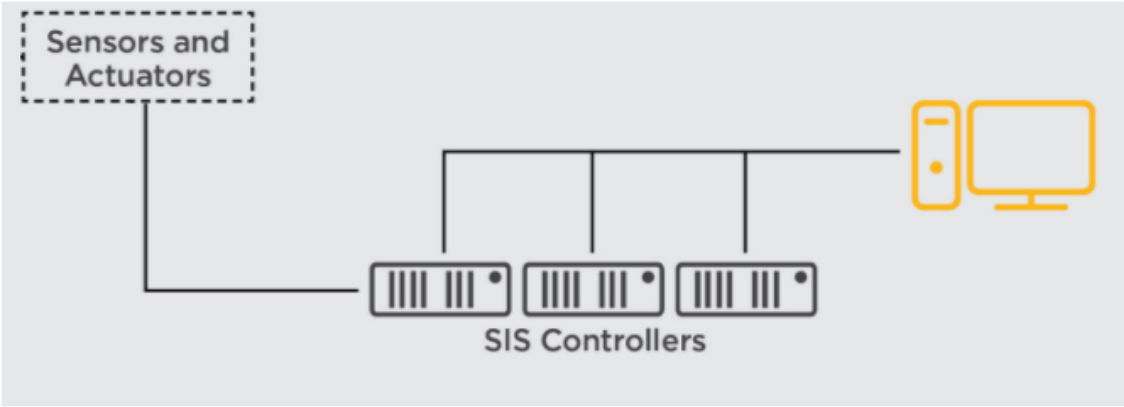
Пример: единый интерфейс Emerson

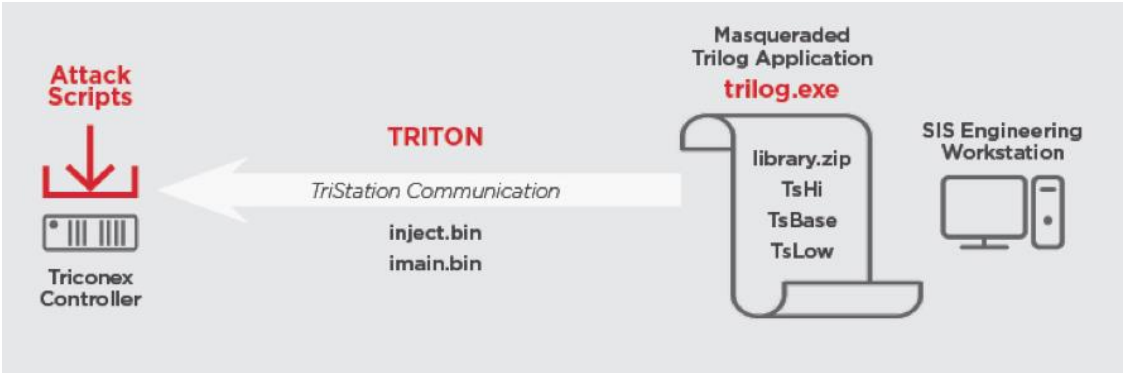
АСУ ТП

ПАЗ



Атака на ПАЗ: TRITON / TRISIS / HATMAN 2017





- ПАЗ Schneider Electric Triconex
- Саудовская Аравия
- IP протокол TriStation
- 0-Day уязвимость в контроллере
- Чтение и запись программы, чтение и запись отдельных функций и запрос состояния контроллера ПАЗ

Возможности атаки:

- Активация ПАЗ для остановки процесса
- Перепрограммирование ПАЗ для пропуска опасного состояния процесса
- Источник: https://goo.gl/yv7P9c

TCIPG: Исследование кибербезопасности I&C на АЭС

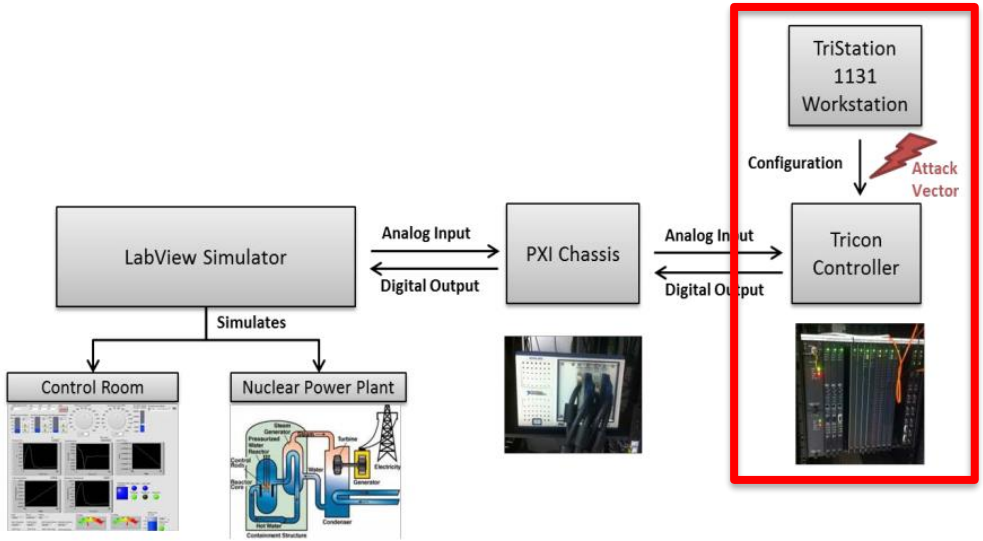


Figure 6. Test Bed Setup for Cyber Security.

Figure 6 depicts the test bed setup. One of the potential attack vectors for the Tricon TMR Controller is during its configuration phase. To configure the Tricon Controller, it needs to be connected to a workstation computer that runs the Tristation 1131 configuration software. Compare to the Tricon controller, the workstation is more susceptible to attacks and compromises due to potential connections to the outside network or accidental infection of viruses through removable devices such as a USB drives. If the workstation that runs the Tristation 1131 software is compromised, then the attacker could hijack either the Tristation 1131 software itself or the communication channel from the Tristation 1131 to Tricon, and use it to send malicious configuration to the Tricon controller.

https://tcipg.org/publications/test-bed-digital-ic-and-cyber-security-npps

Triconex сертифицирован для систем защиты реакторов на АЭС

July 23, 2012 09:00 ET

U.S. NRC Certifies Latest Triconex Controller From Invensys for Use in Nuclear Power Plants

Triple Modular Redundant Tricon System Simplifies Licensing Process, Enables Easier Nuclear Modernization Projects

HOUSTON, TX--(Marketwire - Jul 23, 2012) - Invensys Operations Management, a global provider of technology systems, software solutions and consulting services to the manufacturing and infrastructure operations industries, announced that version 10 of its Triconex® Tricon® controller has been approved for use in safety-related nuclear power plant instrument and control applications by the United States Nuclear Regulatory Commission. In a Safety Evaluation Report (SER) dated April 12, 2012, the NRC indicates that the latest version of the Tricon controller can now be used in safety-related (1E) applications, like reactor protection systems, in U.S. nuclear power plants and U.S. Department of Energy facilities that require licensing or oversight by the NRC. It is the first controller from a dedicated automation vendor to achieve such certification from the NRC and it remains the only triple-modular-redundant system to be qualified.

"The Triconex Tricon system is extremely important to us as we continue to migrate to digital technology, while providing safe, clean, reliable power to our customers in California," said Scott Patterson, program manager for I&C obsolescence for Pacific Gas & Electric, which operates the Diablo Canyon Power Plant in San Luis Obispo, Calif. "Partnering with Invensys, an automation vendor whose core competency is safety systems, gives us an additional layer of protection as we upgrade older safety-related equipment. NRC certification means we can move forward with modernizing and optimizing our plants to ensure their continuous safe operation. We are confident this technology will enhance future upgrades and new designs, as well as ease the licensing process."

Аппаратный ключ не серебряная пуля

There is an important difference between leaving the key in REMOTE or PROGRAM,

in the REMOTE position:

Allows writes to control program variables by TriStation, Modbus masters and external devices. (Download All and Download Change by TriStation are not allowed.)

In the PROGRAM position:

For control program loading and verification. Allows control of the Tricon controller from the TriStation software, including Download All and Download Change. Also allows writes to program variables by Modbus masters and external hosts.

I think the bigger issue is that Triconex communication is not limited to a configured set of equipment, where several other SIS have an approved set of network addresses it permits and on top of that requires a separate login to get access.

I also noticed that many plants keep the key in the PROGRAM mode for fast recovery, however from a security perspective it is bad practice. This new malware shows why.

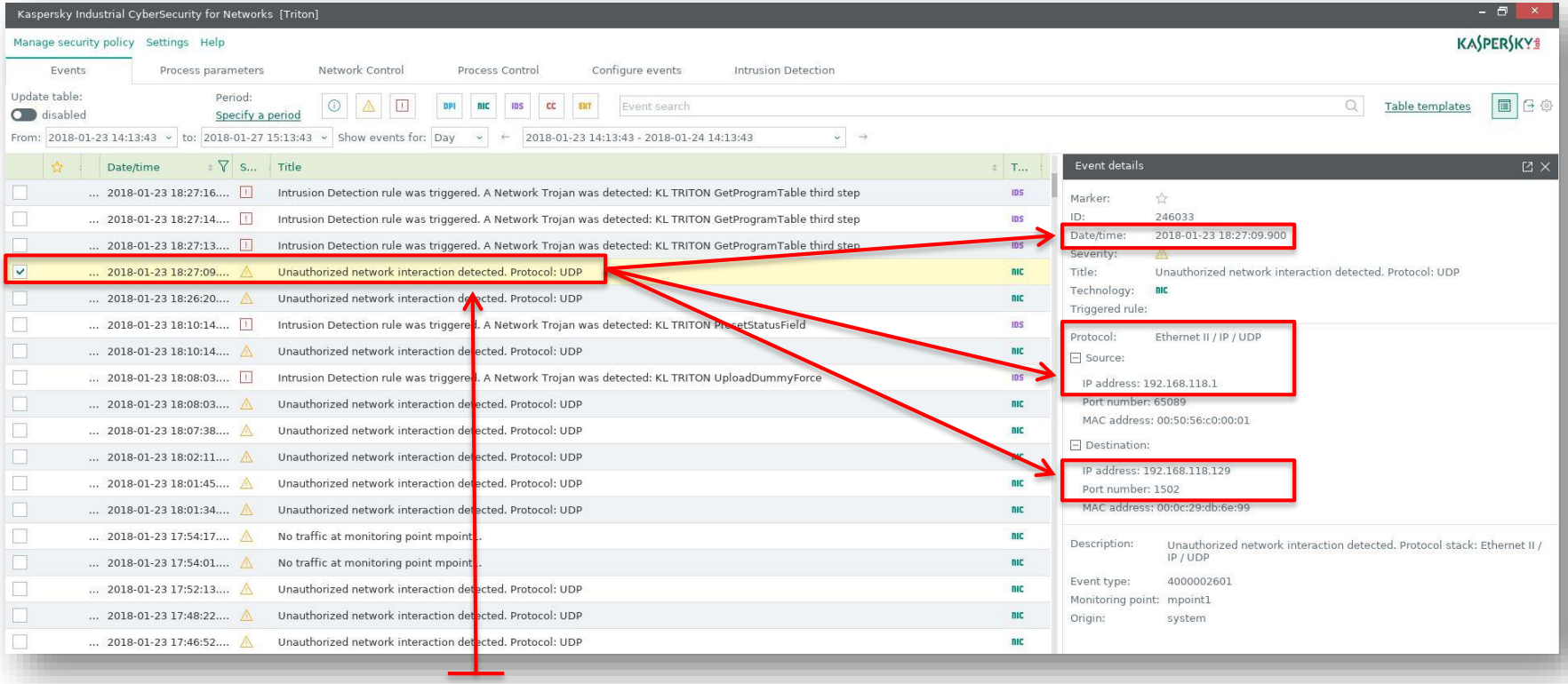
Kind regards,
Sinclair Koelemij

On Dec 17, 2017, at 7:00 PM, scadasec-request@scadasec.email wrote:

Send scadasec mailing list submissions to
scadasec@scadasec.email

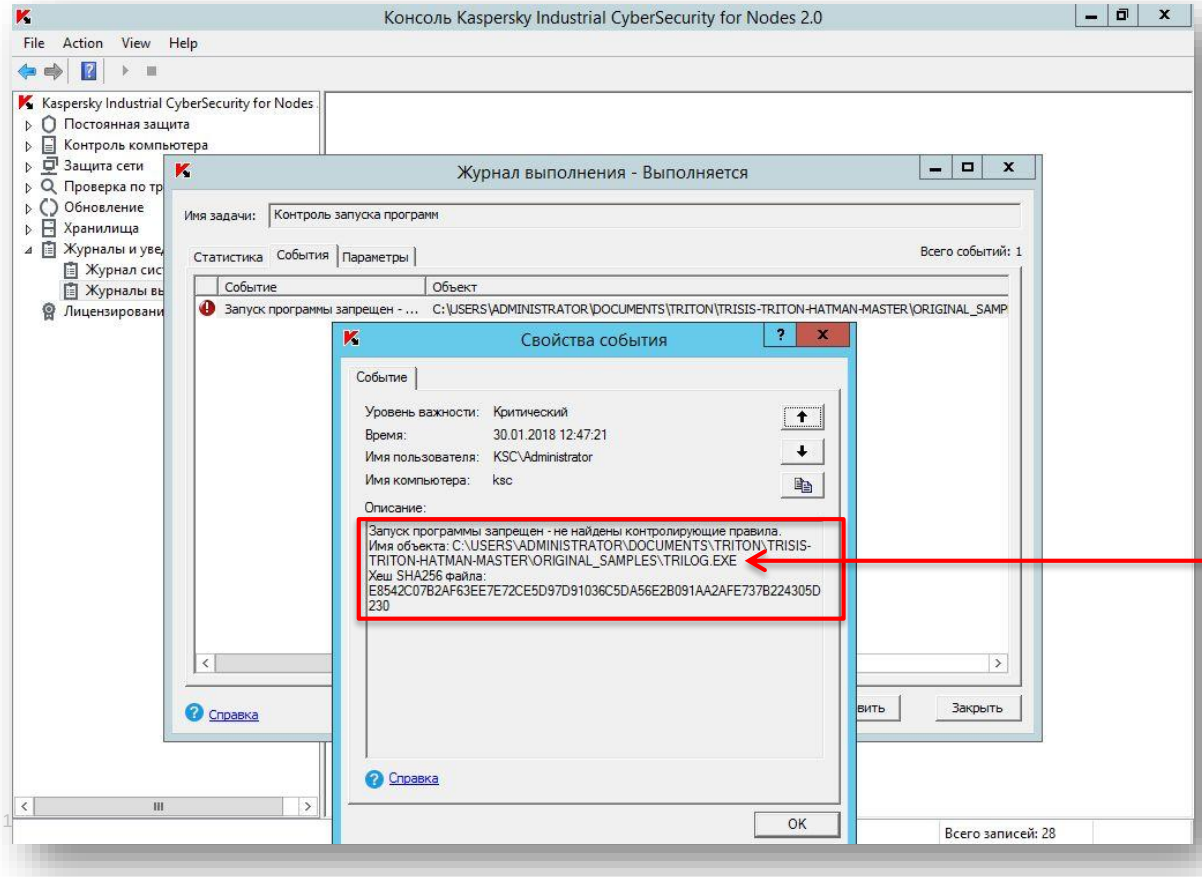
http://scadasec.email/pipermail/scadasec/2017-December/030356.html

KICS for Networks: Белый список коммуникаций vs Triton



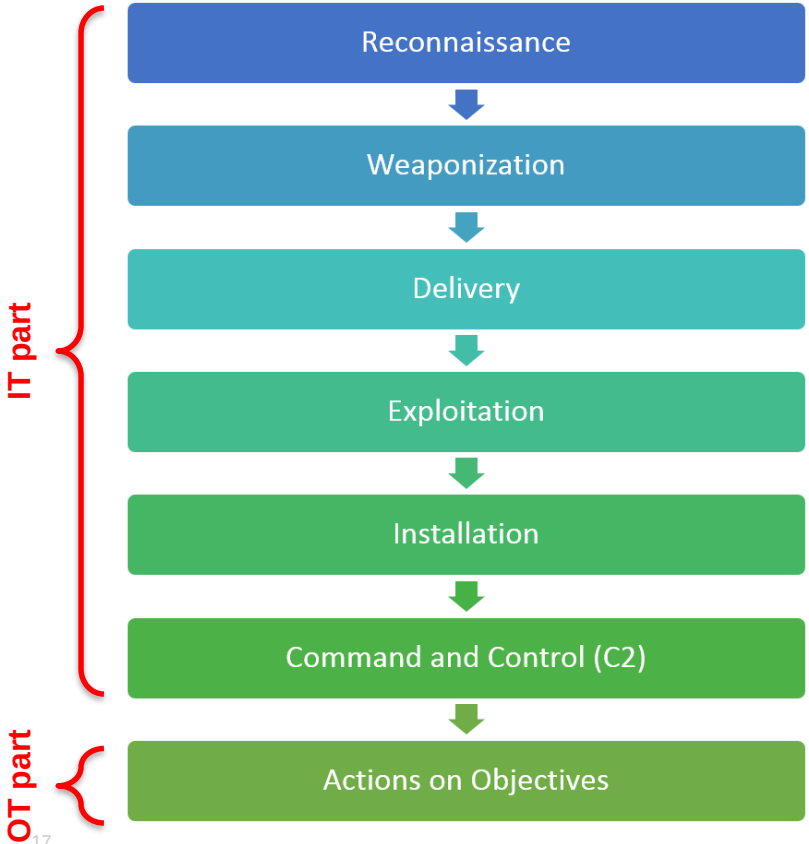
Неразрешенное сетевое соединение в неположенное время
Вне белого списка соединений

KICS for Nodes: Белый список приложений vs Triton



Неразрешенное приложение
Вне белого списка

Cyber Kill Chain / Жизненный цикл кибератаки



1. Поиск и захват OT компонент
2. Анализ конфигураций и изучение процессов
3. Планирование и тестирование атаки
4. Запуск и управление атакой
5. Уничтожение следов

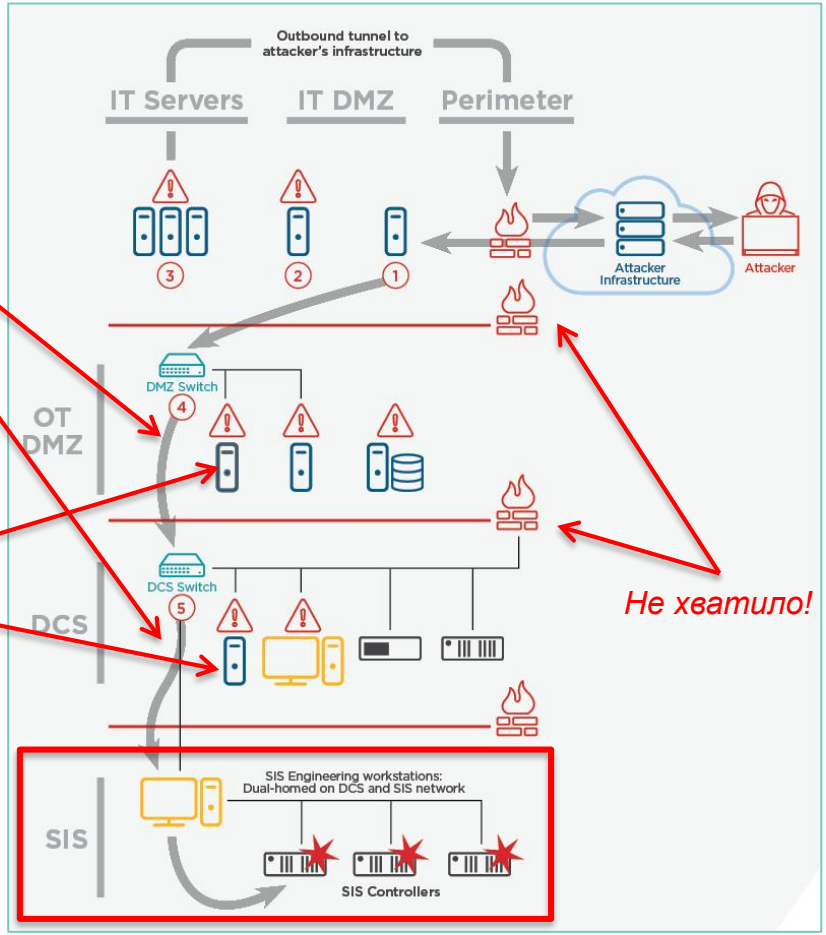
TRITON / Путь атаки

Сетевая активность на разных этапах атаки

- DNS
- SSH
- RDP
- RPC/SMB (PsExec)
- HTTP (Webshell)
- TCP/UDP (Nmap, iPerf)
- VPN

Активность на хостах на разных этапах атаки

- Powershell, Pyton
- SSH clients (Putty/Plinks)
- Netcat/Cryptocat
- Mmikatz, PsExec
- AdExplorer, ShareEnum, PsGetSid
- Nmap, iPerf



Исследовано ранее

Уведомление Schneider Electric

Schneider Electric

Important Security Notification

Detection and Mitigation

Always keep your antivirus tools up to date and ensure you are using the latest antivirus .dat files on the engineering workstation where the TriStation terminal is installed. Signatures for the malware have been distributed to cybersecurity organizations. Schneider Electric has confirmed that major antivirus vendors now include the malware file's signatures and that if detected, the antivirus tool takes action.

Schneider Electric continues to recommend customers always implement the instructions in the "Security Considerations" section in the standard Triconex documentation (i.e., Planning and Installation Guides and TriStation 1131 Developers Guide), which include the following:

- Ensure the cybersecurity features in Triconex solutions are always enabled.
- Safety systems must always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment or the safety network.
- All controllers should reside in locked cabinets and never be left in the "PROGRAM" mode.
- All Tristation engineering workstations should be secured and never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, DVD's, etc. should be scanned before use in the Tristation engineering workstations or any node connected to this network.
- Laptops and PCs should always be properly verified to be virus and malware free before connection to the safety network or any Triconex controller.
- Operator stations should be configured to display an alarm whenever the Tricon key switch is in the "PROGRAM" mode.

https://goo.gl/TCoCHd

Стандарты по кибербезопасности ПАЗ

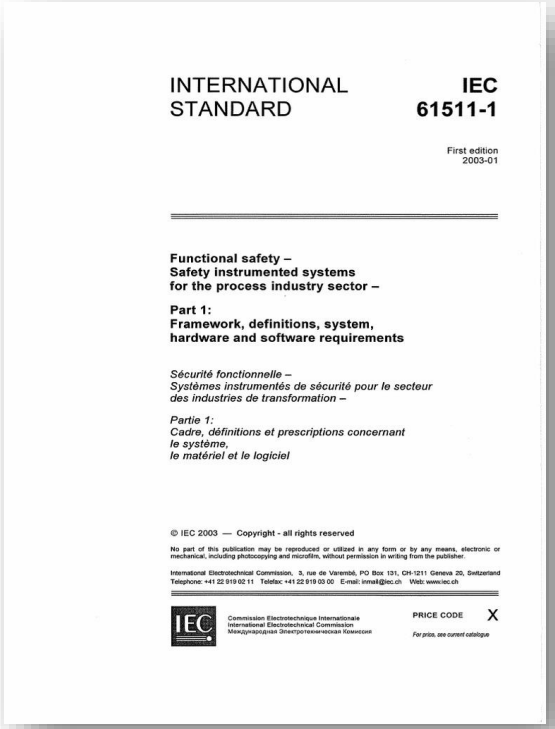
IEC 61511-1:2016

Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements

- Clause 8.2.4: A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.
- Clause 11.2.12: The SIS design shall provide the necessary resilience against the identified security risks

ISA-TR84.00.09-2017

Cybersecurity Related to the Functional Safety Lifecycle


INTERNATIONAL STANDARD

IEC 61511-1

First edition 2003-01

Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and software requirements

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation –

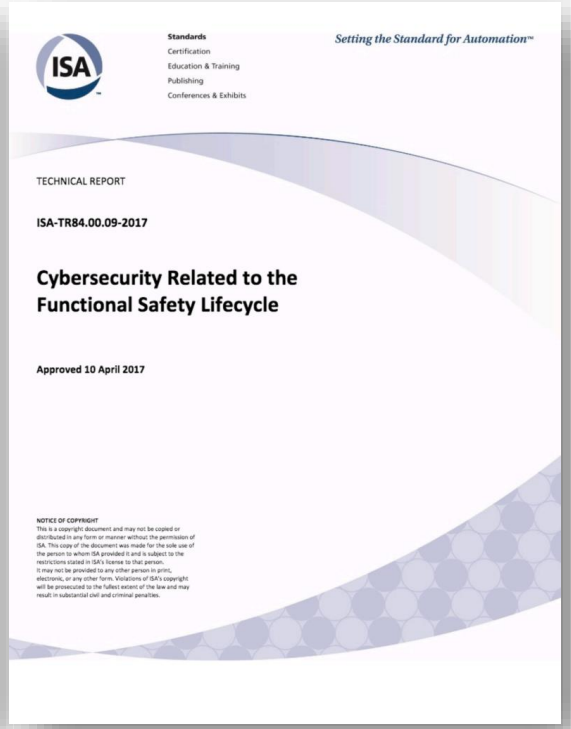
Partie 1: Cadre, définitions et prescriptions concernant le système, le matériel et le logiciel

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE X

For price, see current catalogue


ISA

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.09-2017

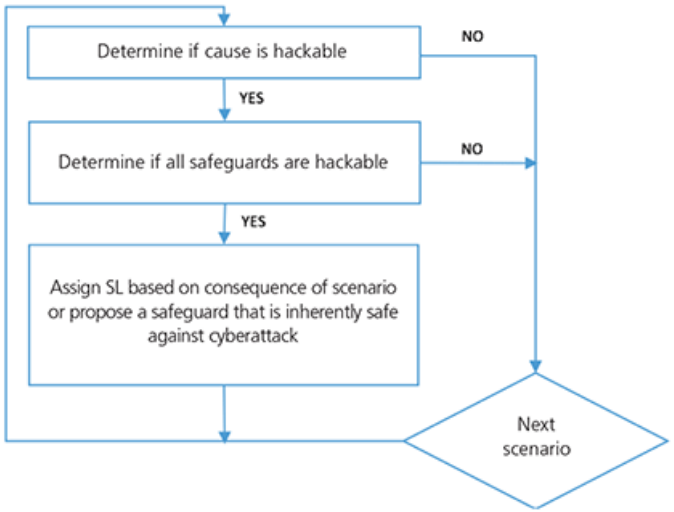
Cybersecurity Related to the Functional Safety Lifecycle

Approved 10 April 2017

Kenexis: Security PHA Review (SPR)

Consequences				
Causes				
Cause	Cause Hackable	Safeguards		Scenario Hackable
		Safeguard	Safeguard Hackable	
1.5.1.1 Failure of control loop LIC-101 such that liquid outlet valve is too much closed.	Yes	8 High level shutdown LT-101B closes inlet valve SDV-101	Yes	Yes
		9 Operator response to high level alarm LT-101A - not independent from control loop failure	Yes	
1.5.1.2 Failure of shutdown valve SDV-102A to the closed position.	Yes	8 High level shutdown LT-101B closes inlet valve SDV-101	Yes	Yes
		9 Operator response to high level alarm LT-101A - not independent from control loop failure	Yes	
1.5.1.3 Slug greater than 90 bbl from production header.	No	9 Operator response to high level alarm LT-101A - not independent from control loop failure	Yes	No
		8 High level shutdown LT-101B closes		

KENEXIS



Источник

For potentially hazardous processes, the results of the process hazard analysis (PHA) and functional safety assessments [20] should be referenced as part of the high-level cybersecurity risk assessment to identify worst-case impacts. Organizations should also take into consideration threat intelligence from governments, sector specific Information Sharing and Analysis Centers (ISACs) and other relevant sources.

ISA

IEC 62443-3-2 [Draft]:Security risk assessment and system design

KASPERSKY

Банк данных угроз безопасности информации ФСТЭК [АСУ ТП]

УБИ.107: Угроза отключения контрольных датчиков — Вид

Описание угрозы Угроза заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путём прерывания канала связи с контрольными датчиками, следящими за параметрами состояния системы, или нарушения работы самих датчиков. При этом система перестанет реагировать как на инциденты безопасности (если отключённые датчики являлись частью системы безопасности, например, датчики движения), так и на другие типы инцидентов (например, при отключении датчиков пожарной сигнализации, повышения давления в гидроагрегатах и др.).
Данная угроза обусловлена слабостями мер защиты информации в автоматизированных системах управления технологическими процессами, а также наличием уязвимостей в программном обеспечении, реализующим данные меры.
Реализация данной угрозы возможна при условии получения доступа (физического или программного) к линиям связи системы безопасности с контрольными датчиками или к самим датчикам

УБИ.176: Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты — Вид

Описание угрозы Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации.
На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации

УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами — Вид

Описание угрозы Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных.
Данная угроза обусловлена наличием у автоматизированной системы управления технологическими процессами программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты.
Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к:
блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия;
нарушению штатного хода технологических процессов;
частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя;
аварийной ситуации в критической системе информационной инфраструктуры

УБИ.204: Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров — Вид

Описание угрозы Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах.
Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации.
Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет

www.bdu.fstec.ru

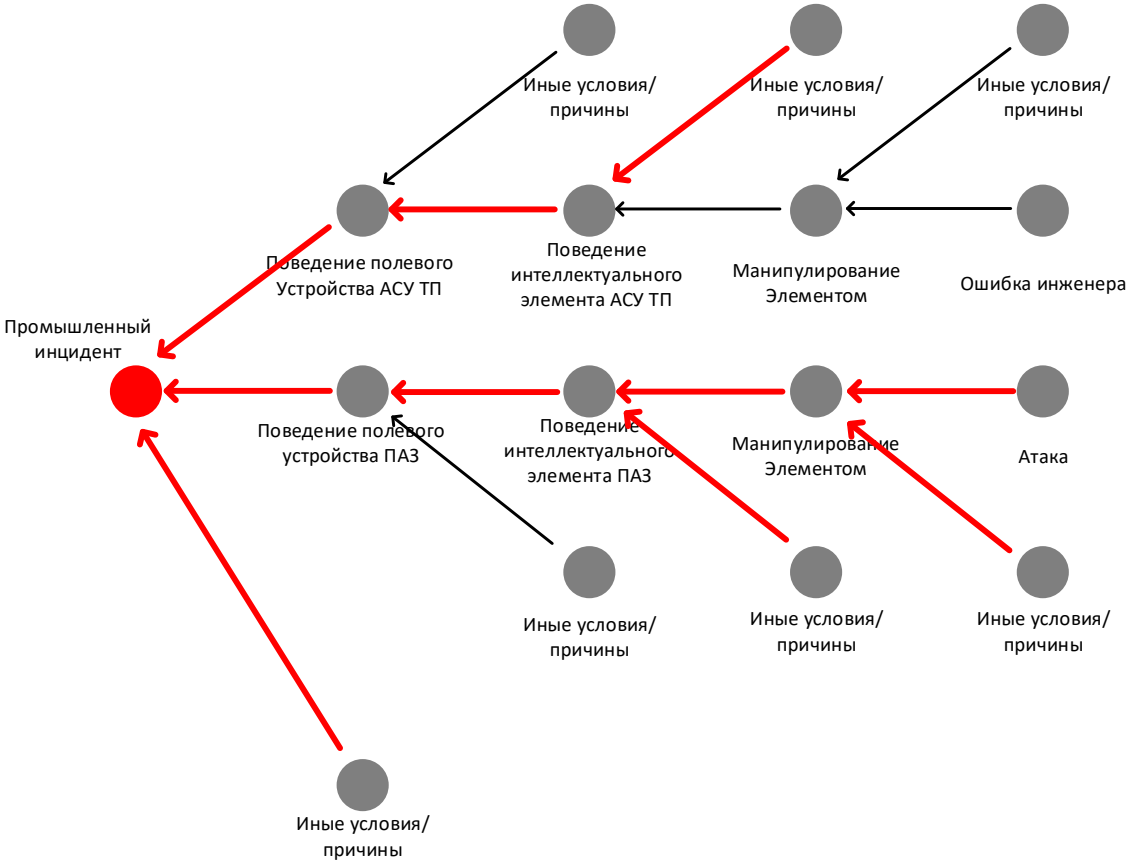
Чеклист NA 163 "Security Risk Assessment of SIS“ 2017

NA 163 описывает кто, как часто и в каких рамках должен проводить оценку риска. Используя чеклист, инженер с базовыми знаниями IT и сетей способен выполнять оценку риска для ПАЗ

1. Gathering the assets/identification of the viewing object
2. System architecture
3. Access and Security
4. Hardening
5. Measures for engineering station, Field Entry Panel, AMS
6. Data
7. Protocols & links
8. Organizations, people and processes

http://www.namur.net/en/publications/news-archive/detail/article/die-na-163-ist-neu-erschienen.html

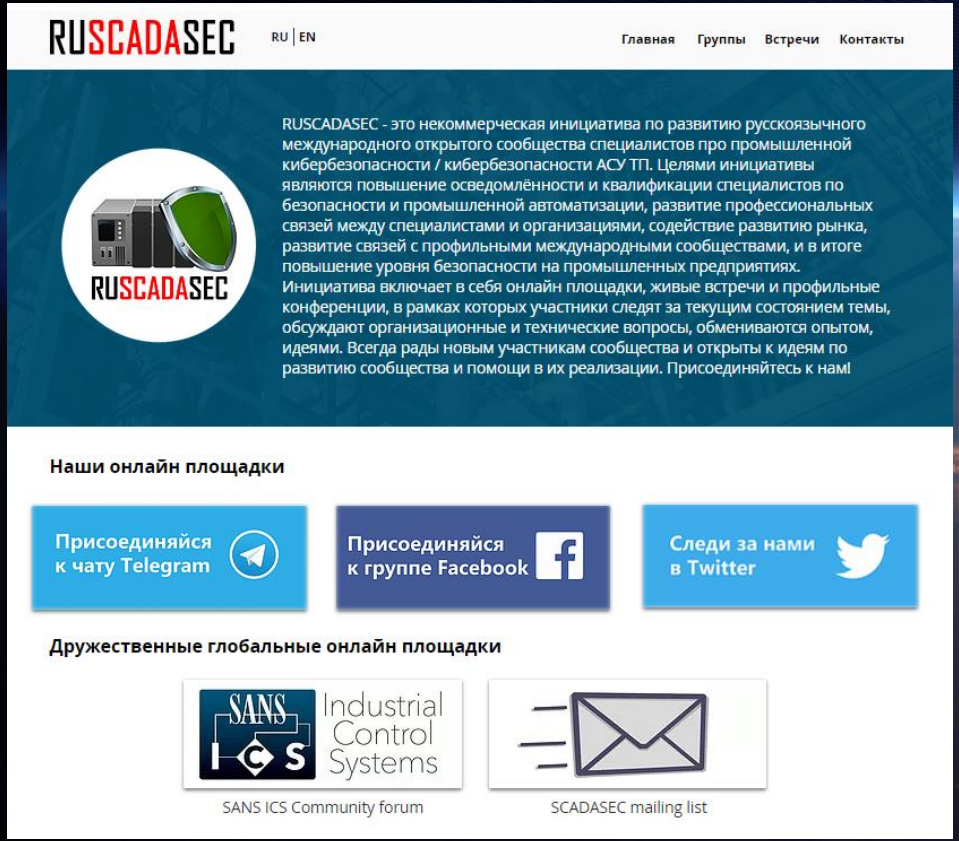
Расследование промышленных инцидентов

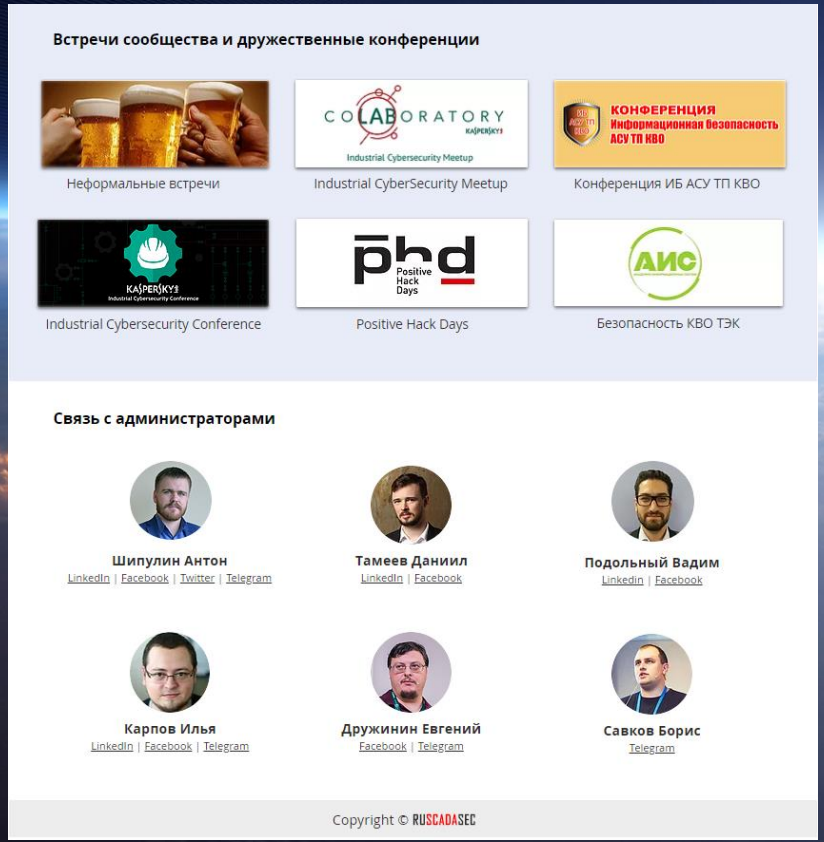


Продолжение следует…

Присоединяйтесь к сообществу

RUSCADASEC.RU





Давайте обсудим?

Антон Шипулин
CISSP, CEH, CSSA
Менеджер по развитию решений по безопасности критической инфраструктуры

Лаборатория Касперского
Москва, Ленинградское шоссе, д.39А, стр.3
T: (495) 797 8700 #1746
Anton.Shipulin@kaspersky.com
www.kaspersky.ru
https://ics.kaspersky.com
https://ics-cert.kaspersky.ru

KASPERSKY lab