Модуль 1. Основи управління кібербезпекою

Лекція 1: Вступ до кібербезпеки ICS/SCADA та ключові поняття

Мета лекції

Сформувати системне розуміння промислових систем керування ICS (Industrial Control Systems — промислові системи керування) та SCADA (Supervisory Control and Data Acquisition — диспетчерське керування і збір даних), обґрунтувати пріоритети кіберзахисту OT (Operational Technology — операційні технології) і пояснити, чому їхній збій має фізичні наслідки для людей, довкілля та економіки.

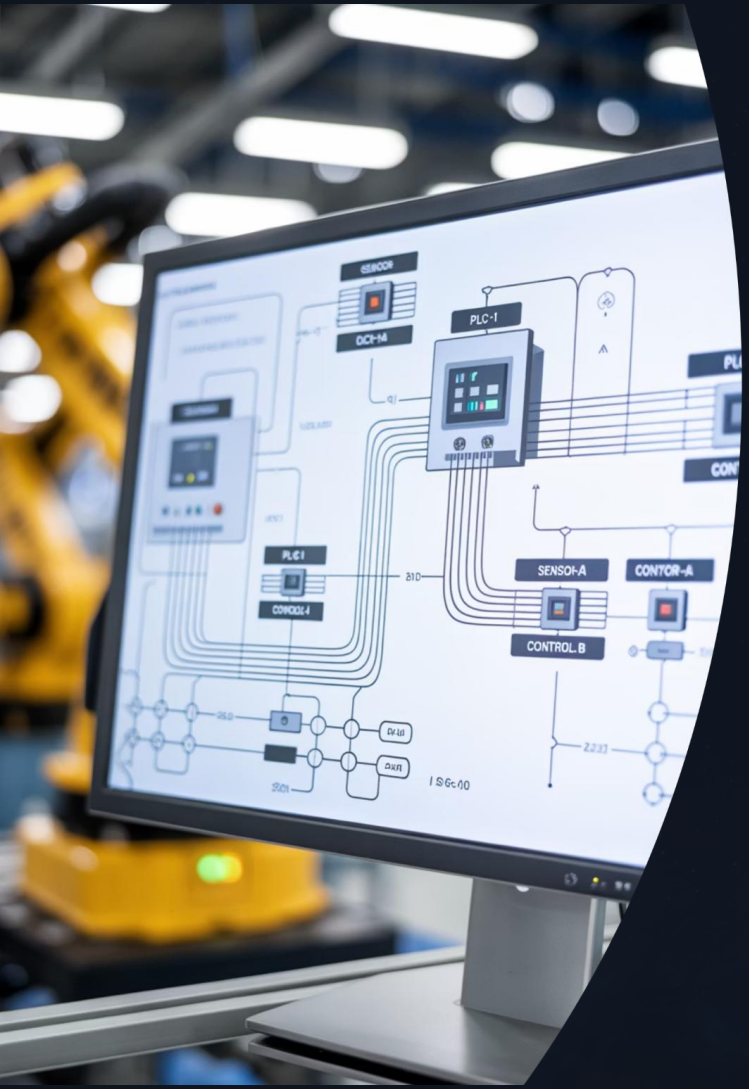
План і очікувані результати

Теми заняття

- Розділ 1. Що таке ICS і SCADA, чому їхня безпека критична
- Розділ 2. Відмінності між кібербезпекою IT та OT
- Розділ 3. Тріада CIA у контексті ICS та модель AIC

Очікувані результати

- Уміння назвати ключові компоненти ICS та їхні ролі
- Розуміння пріоритетів безпеки OT і причин домінування доступності
- Уміння навести приклади інцидентів та зробити висновки для практики



1.1. Що таке ICS і SCADA та чому кібербезпека важлива

1.1.1. Поняття ICS і роль у виробництві

ICS — парасольковий термін для технологічних систем керування процесом, що поєднують датчики, актуатори, контролери, мережі і програмні застосунки

01

Польовий рівень з датчиками і виконавчими механізмами

02

Рівень керування з контролерами і промисловими мережами

03

Рівень диспетчеризації з серверами, історіками та інтерфейсами HMI (Human Machine Interface — людино-машинний інтерфейс)

Завдання ICS

- Стійке і безпечне керування фізичними процесами в реальному часі
- Забезпечення якості, продуктивності та безпеки персоналу

1.1.2. Типи систем керування

SCADA
диспетчеризація і телеметрія на великій території, збір даних з віддалених об'єктів, централізований контроль

DCS (Distributed Control System — розподілена система керування)
глибоко інтегроване керування в межах одного майданчика, ієрархія контролерів і контролю точних параметрів процесу

PLC (Programmable Logic Controller — програмований логічний контролер)
надійний промисловий комп'ютер з виконанням логіки в реальному часі, робота у жорстких умовах

Взаємодія

- DCS і SCADA покладаються на PLC та інші контролери для виконання команд на полі
- Узгодження циклів опитування, пріоритетів і журналювання подій

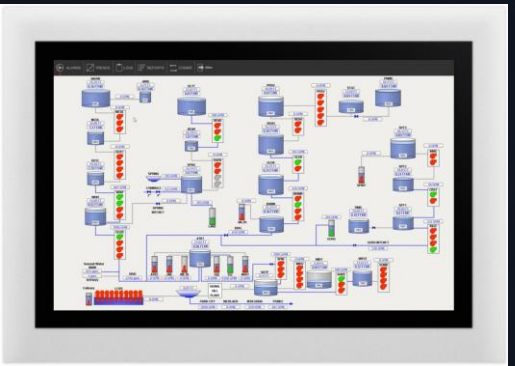
1.1.3. Інші ключові компоненти

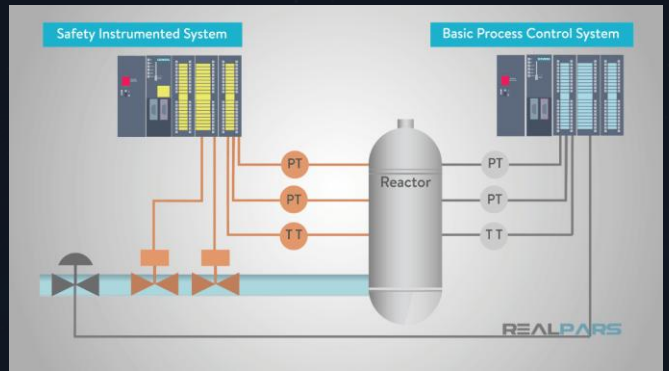
Складові інфраструктури

- RTU (Remote Terminal Unit — віддалена термінальна одиниця) для збору телеметрії і віддаленого керування там, де PLC не виправданий
- HMI для відображення стану, тривог, введення команд і процедур
- SIS (Safety Instrumented System — система функціональної безпеки) для переведення процесу у безпечний стан при відхиленнях
- Data Historian для якісного аналізу тенденцій і діагностики відмов
- IED (Intelligent Electronic Device — інтелектуальний електронний пристрій) у захисті та автоматизації енергетики

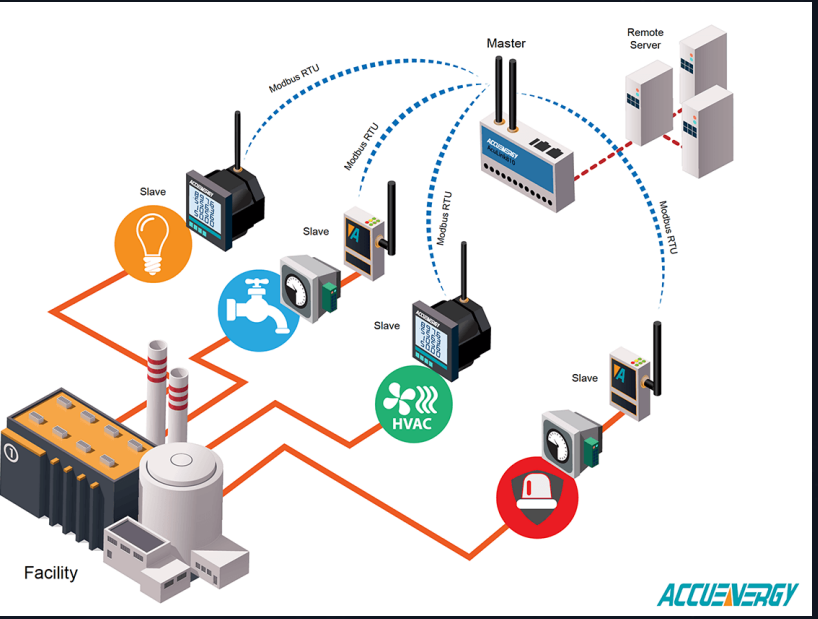
Практичний акцент

Синхронізація часу, відповідальність за межі зон, узгодження журналів подій





1.1.4. Архітектури і канали зв'язку



Мережеві підходи

- Промисловий Ethernet і серійні шини, використання TCP/IP, Ethernet/IP, Modbus, DNP3, PROFINET, BACnet
- Сегментація на зони з кондуїтами за ISA/IEC 62443
- Демілітаризована зона DMZ (Demilitarized Zone — демілітаризована зона) між OT і IT для контрольованого
- Обмежений доступ лише через керовані шлюзи з журналюванням і багатофакторною автентифікацією

Ризики

Бездротові технології і мобільні пристрої збільшують площу атаки і потребують додаткових контролів

1.1.5. Галузі застосування і залежність суспільства

Приклади галузей

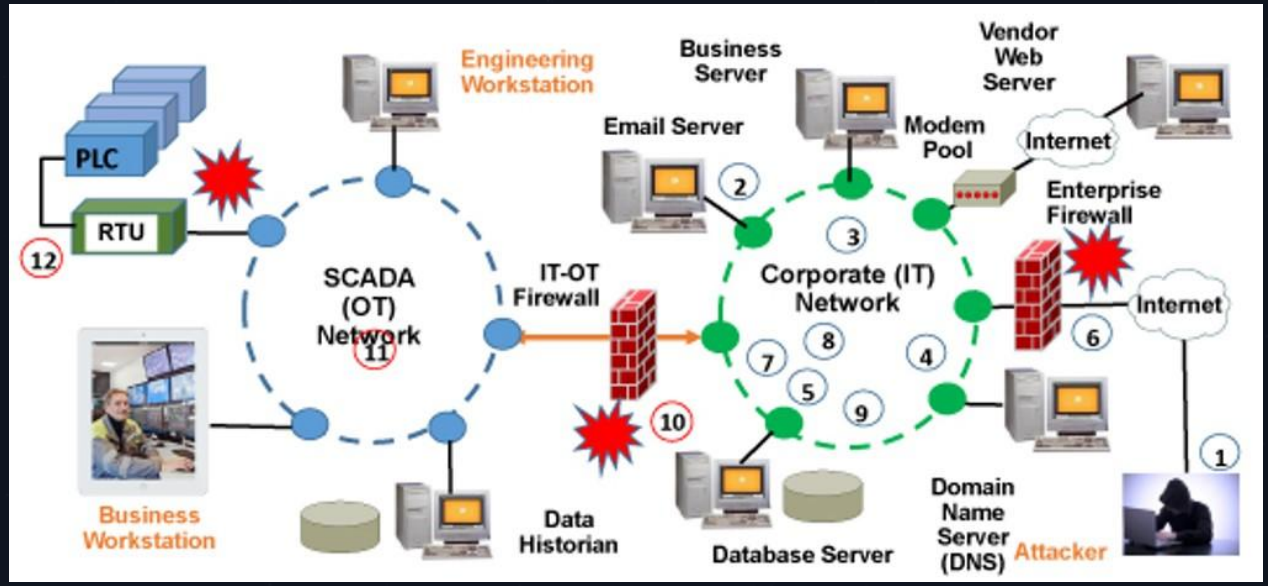
Електроенергетика, нафтогаз і хімія, водоканали, транспорт, металургія, фармацевтика, харчова промисловість, агро

Суспільний вплив

Критична інфраструктура визначає якість життя і безперервність економічних процесів

Каскадні збої

Порушення роботи ICS призводить до каскадних збоїв у суміжних секторах



1.1.6. Чинники критичності кібербезпеки ICS

Причини підвищеної уваги

Вплив на фізичний світ
з потенційними травмами людей і руйнуванням обладнання

Конвергенція IT і OT
з використанням загальновідомих платформ Windows і Linux

Розширення інтеграцій
з корпоративними сервісами, хмарою і аналітикою

Поява IoT
(Internet of Things — Інтернет речей) як множника ризику через велику кількість підключених пристроїв

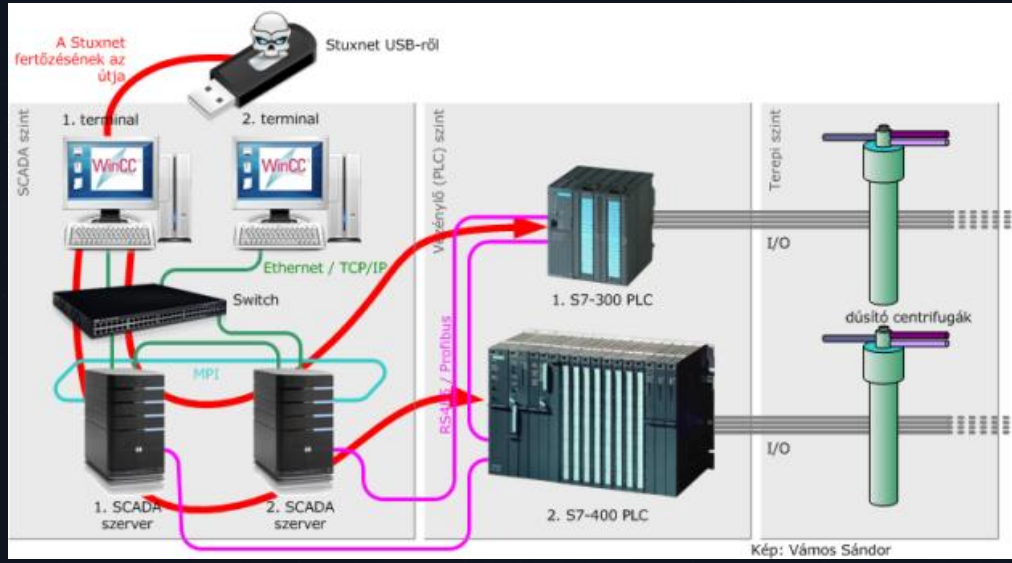
1.7. Інциденти та ключові уроки

Реальні приклади

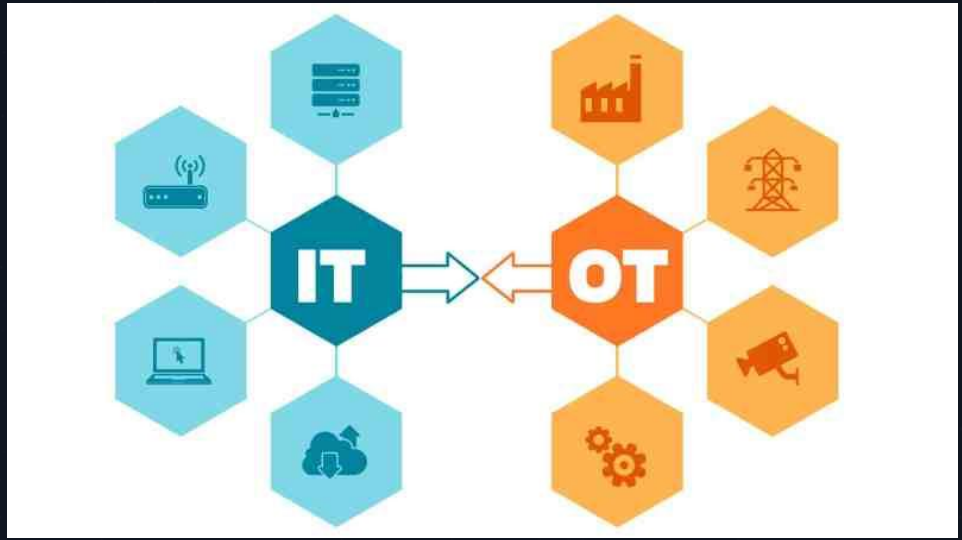
- Stuxnet з маніпуляцією логікою PLC і приховуванням від операторів
- Industroyer з цілеспрямованою роботою по протоколах енергетики
- TRITON або TRISIS з атакою на SIS і ризиком вибуху
- Colonial Pipeline з порушенням бізнес-процесів і зупинкою постачання

Уроки

- Не можна покладатися на ізоляцію без контролів
- Потрібна сегментація, моніторинг і процеси реагування



1.2. Відмінності між кібербезпекою IT та OT



1.2.1. Пріоритети і модель AIC

Порівняння підходів

CIA в IT

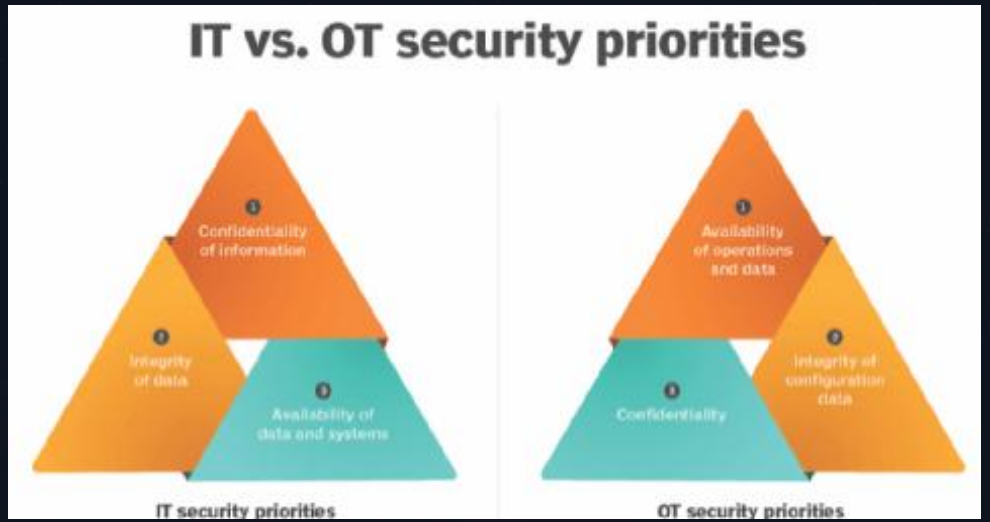
з фокусом на конфіденційність

AIC в OT

з домінуванням доступності, потім цілісності, далі конфіденційності

Обґрунтування

- Зупинка процесу несе матеріальні збитки і ризики для безпеки людей
- Маніпуляція даними здатна спричинити небезпечні дії автоматики
- Конфіденційність промислових даних важлива вибірково з огляду на комерційну та критичну інформацію



1.2.2. Життєвий цикл, зміни і простій

Особливості от

- **Тривалий життєвий цикл**
  IACS (Industrial Automation and Control Systems — системи промислової автоматизації та керування) до двадцяти п'яти років
- **Рідкі зміни і патчі**
  тільки у погоджені вікна після випробувань у стенді
- **Жорсткі вимоги до відновлення**
  і працездатності двадцять чотири години на добу

Практика

Плани відкату, збереження конфігурацій, контроль впливу на процес перед релізом

1.2.3. Ресурси, реальний час і протоколи

Технічні відмінності

- Контролери з RTOS або мінімалістичними ОС, що обмежує сучасні засоби захисту
- Протоколи на кшталт Modbus і DNP3 історично без шифрування і автентифікації
- Висока чутливість до затримок і джитеру, що впливає на вибір IDS і політик фільтрації

Компенсація

Білий список команд, опитування з контролем послідовності, ізоляція критичних потоків

1.2.4. Архітектурні припущення і зони

Архітектура безпеки

01

Відмова від припущення повної ізоляції цеху

02

Побудова зон і кондуїтів за ISA/IEC 62443

з міжмережевими екранами і проксі

03

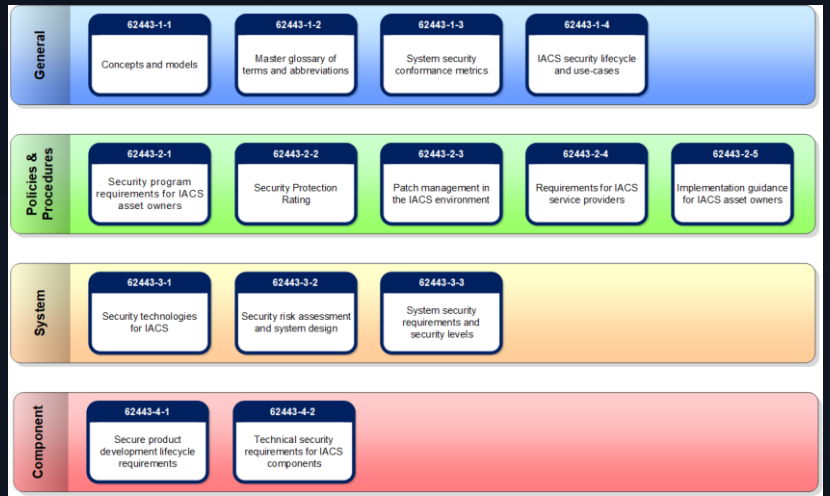
DMZ для інтеграції з IT і хмарою

заборона прямих з'єднань OT в Інтернет

04

Керований віддалений доступ

з журналюванням і багатофакторною автентифікацією



1.2.5. Практичні наслідки і рекомендації

Керівні принципи

- Неможливо механічно переносити IT-контролі в OT без урахування реального часу
- Спільні плейбуки реагування і крос-навчання команд IT та OT

Базові контролі

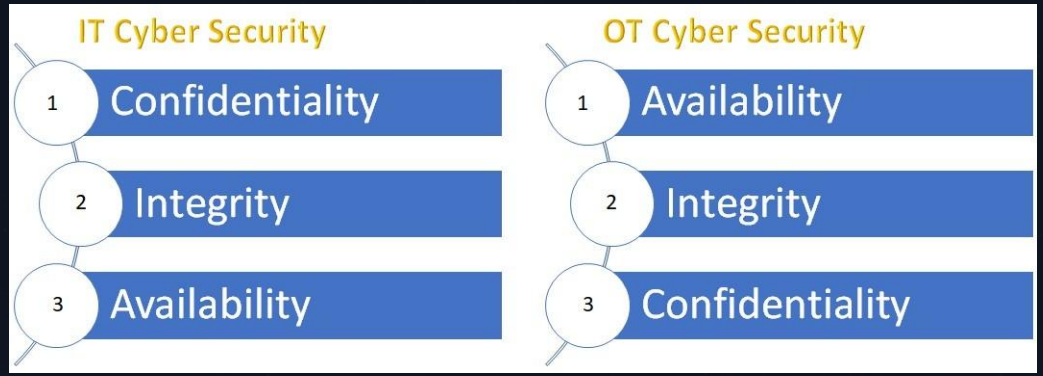
Інвентаризація активів і прошивок

Сегментація і мінімальні привілеї

Вайтлістинг застосунків і драйверів

Резервне копіювання конфігурацій і перевірка відновлення

1.3. Тріада CIA у контексті ICS та модель AIC



1.3.1. Доступність у промислових системах

Значення доступності

Гарантована готовність систем і даних для авторизованих користувачів і алгоритмів

Причини домінування

- Фізична безпека, якість продукції, екологічні вимоги
- Висока вартість простою і запуску процесу після зупинки

Практичні засоби

Надлишковість

мереж і обладнання, відмовостійкі топології, гарячі резерви

Планування

вікна змін, тестові середовища, контроль навантаження

Відновлення

підписані резервні копії та сценарії відновлення

1.3.2. Цілісність і конфіденційність у ICS

Цілісність

Точність телеметрії і довіра до команд керування є критичними

Контролі

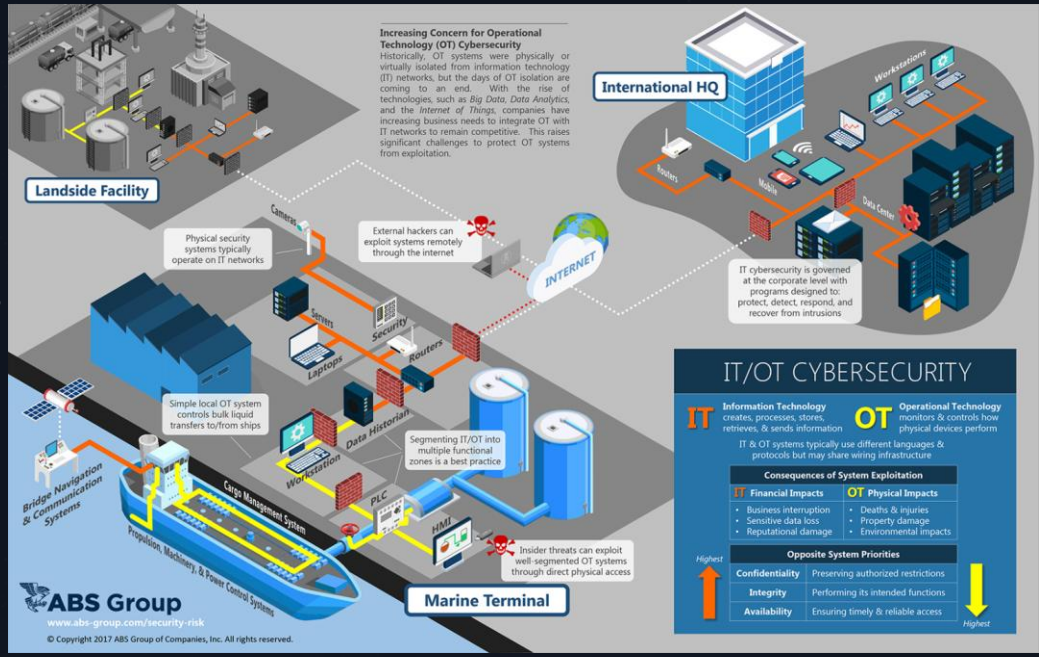
- Взаємна автентифікація пристроїв
- OPC UA (Open Platform Communications Unified Architecture) з шифруванням і сертифікатами
- Підпис конфігурацій, білий список операцій, контроль змін

Конфіденційність

Пріоритет нижчий, але важлива для схем мереж, правил брандмауера, планів відключень і комерційно значущих даних

Контролі

- Сегментація, рольовий доступ
- Шифрування трафіку
- Фізичний захист документації



1.3.3. Практичні кроки впровадження AIC

Реалізація в політиках

01

Класифікація функцій за критичністю доступності

02

Вимоги до цілісності конфігурацій і журналів

03

Політика обробки конфіденційних артефактів SCADA

Рекомендації

- Орієнтуватися на ISA/IEC 62443 для архітектури і процесів
- Використовувати керівництво NIST SP 800-82 для добору контролів у SCADA, DCS і PLC

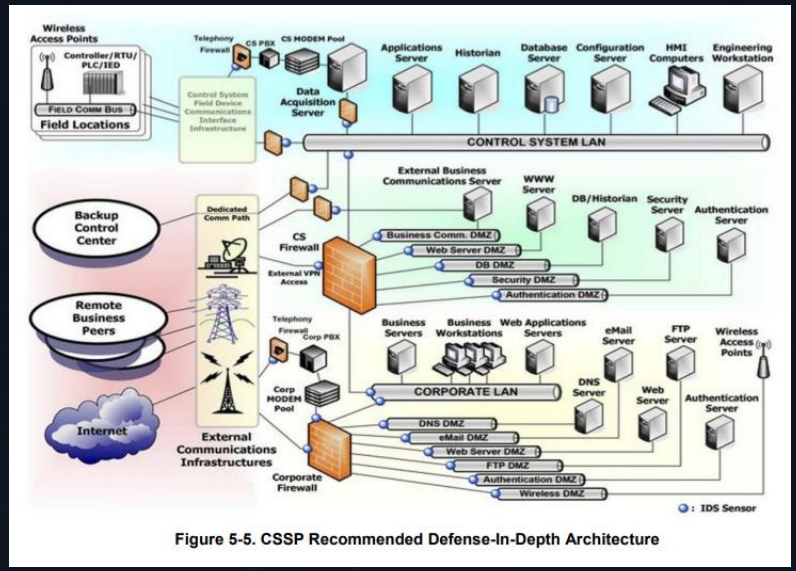


Figure 5-5. CSSP Recommended Defense-In-Depth Architecture

1.4. Підсумки і перевірочний чек-лист

- ICS керують фізичними процесами, тому моделі безпеки мають пріоритет доступності
- Конвергенція IT і OT робить відомі IT-загрози релевантними для виробництва
- Потрібні архітектурні, процесні і технологічні захисти з урахуванням реального часу

Чек-лист впровадження

1. **Інвентаризація активів і зонування з кондуїтами**
2. **DMZ між OT і IT, керований віддалений доступ**
3. **Резервне копіювання конфігурацій і регулярні тести відновлення**
4. **Вайтлістинг і контроль цілісності прошивок**
5. **Патч-менеджмент через тестові середовища**
6. **Постійне навчання персоналу і спільні плейбуки реагування**

Список використаних джерел

1. Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security (2nd ed.). CRC Press.

2. Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-Security of SCADA and Other Industrial Control Systems. Springer.

3. Shaw, W. T. (2020). Cybersecurity for SCADA Systems (2nd ed.). PennWell Books.

4. Brooks, C. J., & Craig Jr., P. A. (2022). Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. Wiley.

5. Kouremetis, M. (2014). Defending a SCADA System with the Snort IDS [Presentation]. ECSSE Department.

6. National Telecom Regulatory Authority (NTRA). (2022). IoT Cyber Security Framework. EG-CERT.

7. Emerson. (2021). Industrial Security in SCADA Systems: IEC 62443-3-3 Certification. Emerson Automation Solutions.

8. Krotofil, M. (2023). Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle. Technical White Paper.

9. UtilSec, LLC. (2024). Getting Started in ICS/OT Cyber Security: Lab Manual. UtilSec.

Дякую за увагу!