Модуль 3. Основні принципи мережевого захисту для ICS/SCADA та інтеграції промислових систем в IT-інфраструктуру

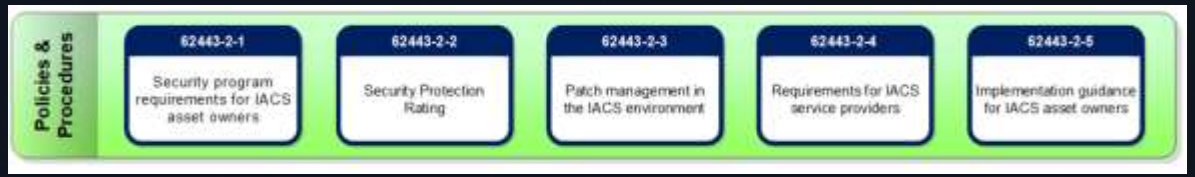
Лекція 1: Безпечна мережева архітектура та сегментація

Мета лекції

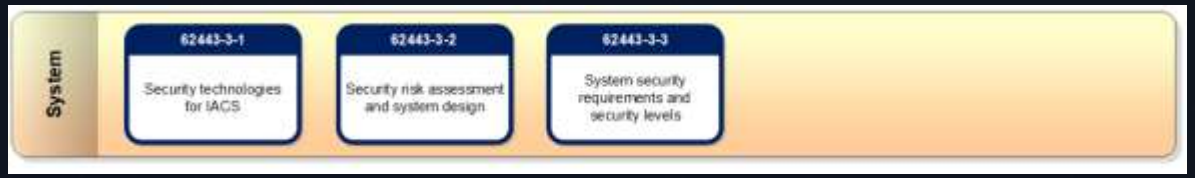
Метою цієї лекції є формування системного розуміння того, як побудувати безпечну архітектуру промислових мереж та інтегрувати їх у корпоративне середовище без шкоди для надійності процесів.

- [ ] Пояснити відмінності між IT та OT підходами до безпеки
- [ ] Розглянути модель Пердью та стандарти ISA/IEC 62443 як основу для проєктування
- [ ] Вивчити методи сегментації мережі: VLAN, міжмережеві екрани, DMZ
- [ ] Зрозуміти роль посилення систем, управління конфігураціями та патчами
- [ ] Закріпити практичні рекомендації щодо мінімізації ризиків та підвищення стійкості

1.1. Модель Пердью та зони й канали ISA/IEC 62443



Модель Пердью (Purdue Model) є ієрархічною моделлю, яка описує архітектуру промислових систем контролю. Вона стала міжнародним стандартом для взаємозв'язку IT- та OT-мереж.



1.1.1. Структура моделі Пердью

Рівень 0

Процеси та датчики/виконавчі механізми

Рівень 1

Базове керування процесами

Рівень 2

Нагляд та керування

Рівень 3

Операційне управління

Рівень 4

Бізнес-планування

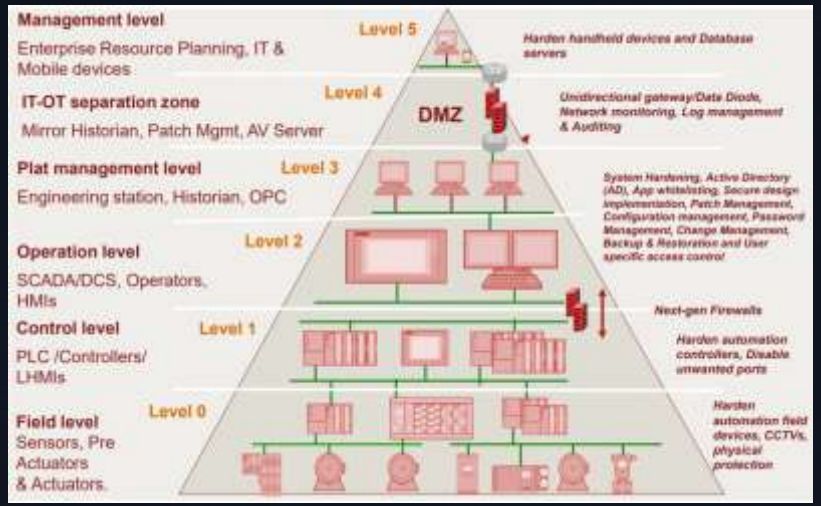
Рівень 5

Бізнес, планування та логістика

Модель також визначає типи обладнання, мережеві підключення та бізнес-операції, що відбуваються на кожному рівні.

1.1.2. Стандарти ISA/IEC 62443

Стандарт ISA/IEC 62443, раніше відомий як ISA 99, є де-факто світовим стандартом безпеки мереж промислового керування (ICS). Він був розроблений Міжнародним товариством автоматизації (ISA) та прийнятий Міжнародною електротехнічною комісією (IEC).



> Серія стандартів ISA/IEC 62443 вважається "золотим стандартом" для програм кібербезпеки в середовищах ICS/OT.

1.1.3. Структура серії IEC 62443

Серія IEC 62443 складається з 14 документів, розподілених на чотири основні рівні:

Загальний рівень (General)

Представляє загальні концепції та моделі серії. Наприклад, технічний звіт 62443-1-2 містить глосарій термінів та скорочень.

Рівень системи управління

Описує необхідні політики та процедури для впровадження системи управління кібербезпекою (CSMS).

Рівень системи

Описує вимоги кібербезпеки для системи в середовищі IACS.

Компонентний рівень

Описує вимоги кібербезпеки для окремих компонентів в середовищі IACS.

1.1.4. Зони безпеки (Security Zones)

Зони безпеки - це фізичні або логічні угрупування активів, які мають спільні вимоги до безпеки та відокремлюють критичні компоненти систем керування.

Розподіл активів на зони є першим кроком у фазі оцінювання життєвого циклу кібербезпеки.

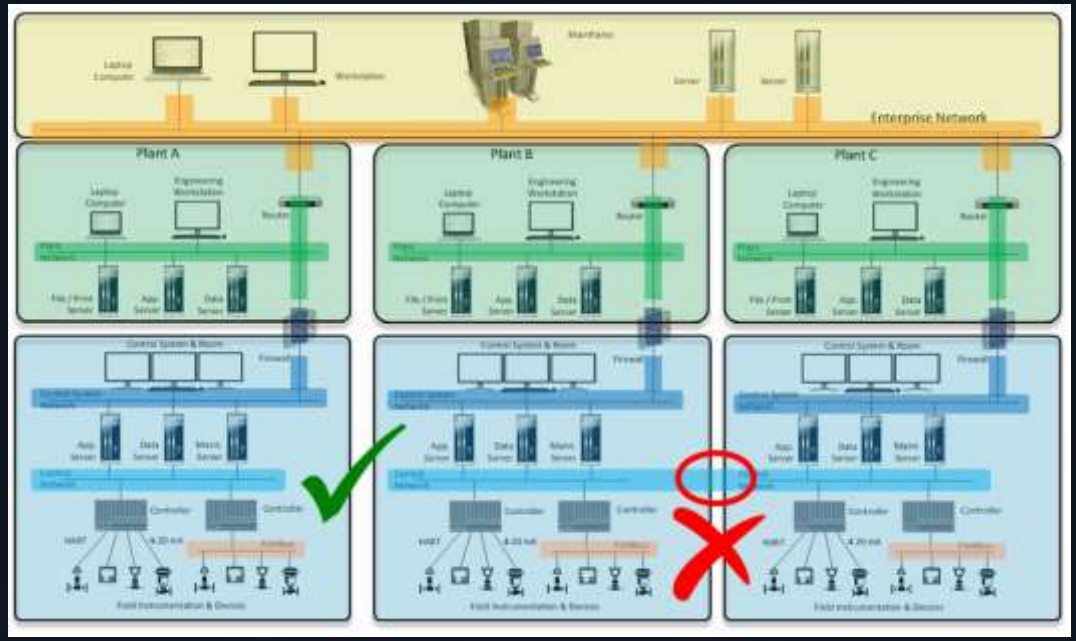
Fig. 1 Zones in Industrial Control System

1.1.5. Канали (Conduits)

Канали - це особливий тип зони безпеки, який групує дані, що логічно поєднуються у потоки інформації всередині та поза зоною.

Канал контролює доступ до зони, протидіючи атакам (наприклад, DoS, шкідливому програмному забезпеченню) та захищаючи цілісність і конфіденційність мережевого трафіку.

Канали можуть бути реалізовані як окремий сервіс (наприклад, мережа Ethernet) або як декілька носіїв даних.



1.1.5. Висновки щодо моделі Пердью та ISA/IEC 62443

Модель Пердью та стандарти ISA/IEC 62443 із їхніми концепціями зон та каналів є фундаментальними для побудови надійної архітектури безпеки промислових систем.

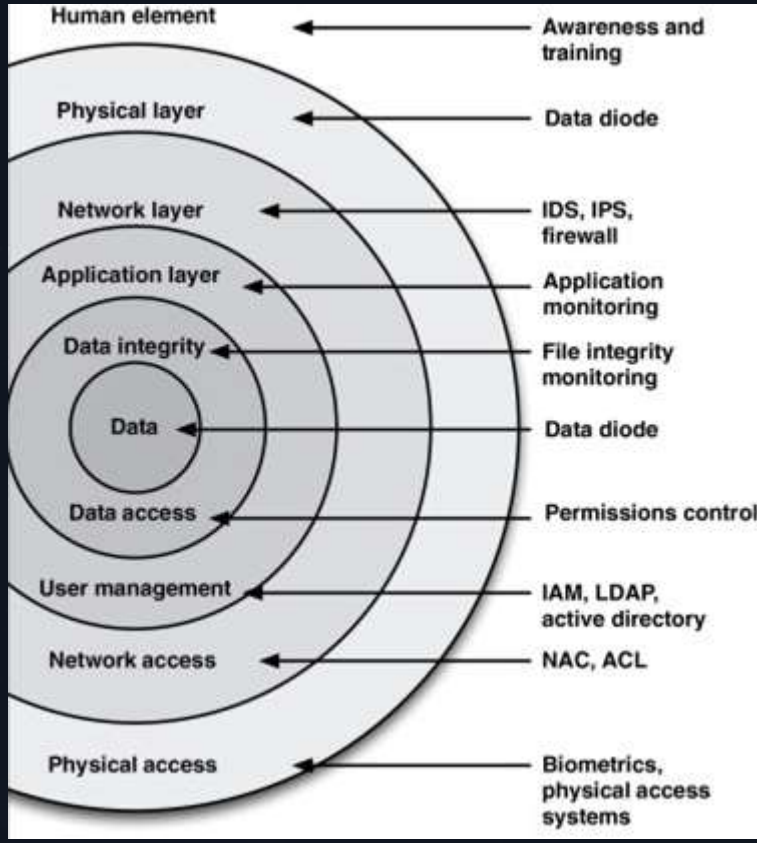
- Рекомендується використовувати ці моделі як основу для стратегічного планування кібербезпеки
- Вони забезпечують структурований підхід до ідентифікації, групування та захисту активів
- Чітке визначення зон та каналів дозволяє ефективно застосовувати захисні заходи та знижувати ризики

1.2. Методи сегментації мережі

Сегментація мережі є критично важливим заходом безпеки, що допомагає ізолювати критичні системи та контролювати трафік.

При проектуванні мережевої архітектури для ICS рекомендується відокремлювати мережу ICS від корпоративної мережі, оскільки характер трафіку на них різний, і проблеми безпеки або продуктивності в корпоративній мережі не повинні впливати на мережу ICS.

Ця стратегія є частиною підходу "захист в глибину“ (Defense-in-Depth).



1.2.1. VLAN (Virtual Local Area Networks)

Визначення та призначення

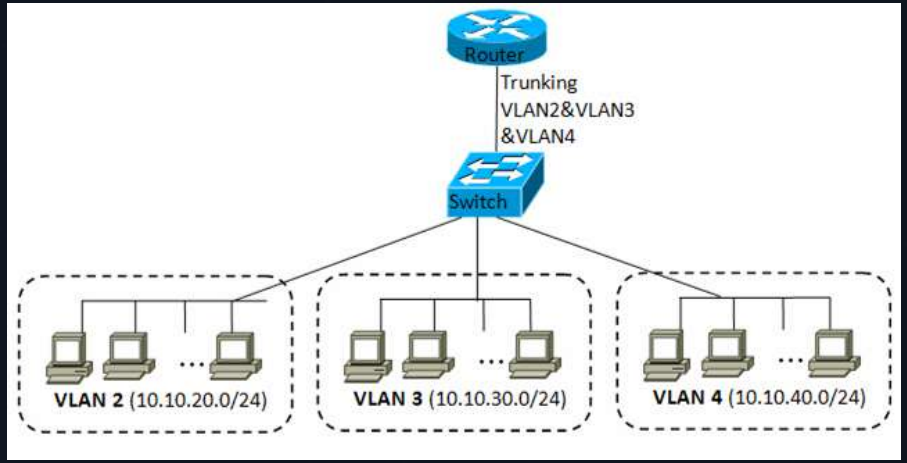
Віртуальні локальні мережі (VLAN) – це логічно захищені мережеві сегменти, які обмежують видимість мережевого трафіку, дозволяючи пакетам переміщуватися лише між призначеними портами.

Застосування в ICS

VLAN ефективно розгортаються в ICS-мережах, де кожна автоматизаційна комірка може бути призначена одній VLAN для обмеження надмірного трафіку.

Реалізація

VLAN створюються за допомогою керованих комутаторів. Вони можуть використовуватися для спільної комутованої мережі Ethernet або фізично приватної локальної мережі.



1.2.2. Міжмережеві екрани (Firewalls)

Міжмережеві екрани є основними компонентами безпеки, що контролюють вхідний та вихідний мережевий трафік на основі встановлених правил безпеки.

Роль та призначення

Використовуються для реалізації захисту периметра та сегментації мережі

Розміщення

Зазвичай розміщуються між корпоративною мережею та мережею керування

Виклики

Неправильне налаштування може відкрити доступ для неавторизованих осіб та шкідливого ПЗ

⚠ Важливо зазначити, що не всі міжмережеві екрани підтримують ICS-специфічні протоколи.

1.2.3. Типи міжмережевих екранів

Application Proxy Firewalls

Міжмережеві екрани на рівні додатків

Packet-Inspection Firewalls

Міжмережеві екрани з інспекцією пакетів

Stateful Inspection Firewalls

Міжмережеві екрани з перевіркою стану

Industrial Protocol-Aware Firewalls

Міжмережеві екрани, що розуміють промислові протоколи

1.2.4. Демілітаризовані зони (DMZ)

Демітаризована зона (DMZ) – це ізольований мережевий сегмент, який слугує буфером між внутрішньою (довіреною) та зовнішньою (недовіреною) мережами.

У контексті ICS/OT DMZ призначена для безпечного розділення IT- та OT-мереж.

Зазвичай DMZ розташовується між IT- та OT-мережами.

1.2.5. Найкращі практики для DMZ

> Рекомендується, щоб OT-мережа ініціювала зв'язок з IT-мережею (наприклад, для передачі даних від дата-історіків), а не навпаки.

Це зменшує ризик того, що зловмисник, скомпрометувавши IT-мережу, зможе ініціювати з'єднання безпосередньо в OT-мережу.

Це є критично важливим для контролю трафіку та запобігання несанкціонованому доступу.

1.2.6. Висновки щодо сегментації мережі

Ефективна сегментація мережі за допомогою VLAN, міжмережевих екранів та DMZ є фундаментальною для захисту ICS/OT.

Багатошаровий захист

Створення декількох рівнів безпеки

Зменшення поверхні атаки

Обмеження точок доступу

Контрольований обмін даними

Забезпечення безпечної комунікації

1.3. Посилення (hardening) мережевих пристроїв та операційних систем

Посилення (hardening) – це процес зменшення поверхні атаки шляхом видалення або відключення непотрібних служб, утиліт та додатків на мережевих пристроях та операційних системах.

Це є ключовим для захисту систем від вразливостей.

1.3.1. Видалення або відключення непотрібних служб

Основний принцип

Слід видаляти або відключати всі файли та програми, які не є критично необхідними для функціонування промислової системи контролю.

Мережеві інтерфейси

Рекомендується вимикати бездротові інтерфейси на комп'ютерах, підключених до локальних мереж з критично важливими активами. Найкраще фізично видаляти відповідні схемні плати або видаляти програмне забезпечення драйверів.

Порти

Блокування непотрібних портів в операційних системах є ефективним заходом посилення. Відкриття таких портів, як FTP (порт 21), може призвести до перехоплення незашифрованих даних.

1.3.1. Безпечні конфігурації

Неправильні або небезпечні конфігурації, модифіковані з початкових налаштувань або адаптовані до середовища замовника, є значною загрозою.

Важливо, щоб власники/оператори були обізнані з правильними конфігураціями безпеки.

1.3.2. Управління конфігураціями

Контроль доступу

Необхідно підтримувати жорсткий контроль над точками доступу до ICS, включаючи сильну автентифікацію, фізичну безпеку та контроль знімних носіїв.

Доступ до діагностичних дисплеїв та можливість маніпулювати налаштуваннями також повинні контролюватися за допомогою відповідних механізмів авторизації.

Базові конфігурації

NIST SP 800-53 CM-2 підкреслює необхідність розробки, документування та підтримки актуальних базових конфігурацій інформаційних систем.

Ці конфігурації повинні містити інформацію про компоненти системи, мережеву топологію та логічне розміщення компонентів.

1.3.3. Документація архітектури систем

> Документація архітектури систем повинна бути строго контрольованою в IT/OT-відділах організації, з обмеженим доступом лише для уповноваженого персоналу на основі принципу "потреби знати".

Зміни в системі вимагають створення нових базових конфігурацій.

1.3.4. Управління патчами

Управління патчами є критично важливим для кібербезпеки, оскільки патчі усувають вразливості, виявлені постачальниками обладнання.

01

Оцінка патчів

Потенційні патчі повинні бути оцінені до встановлення в систему

02

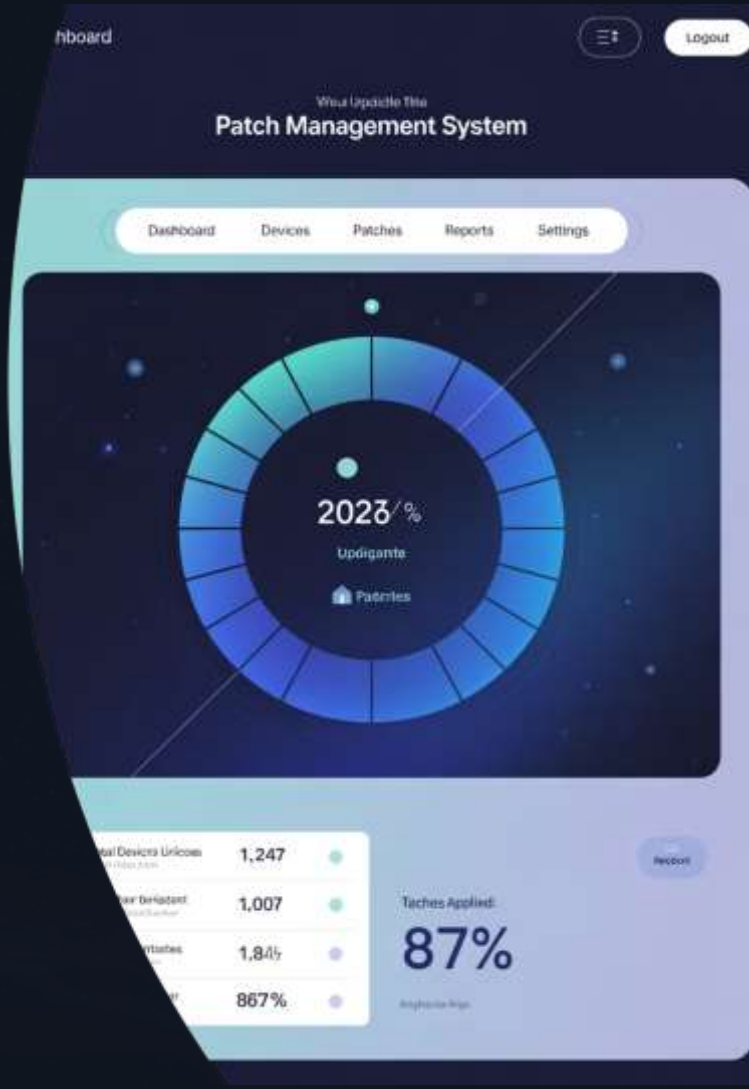
Тестування

Рекомендується тестувати патчі в "пісочниці" (sandbox) перед розгортанням

03

Розгортання

Встановлення патчів у виробничій мережі після успішного тестування



1.3.5. Графік встановлення патчів

Традиційно компанії з ICS оновлювали програмне забезпечення під час планових відключень системи, але вимоги кібербезпеки вимагають можливості встановлення патчів безпеки між запланованими відключеннями.

Процес управління патчами спрощується, якщо компанії підтримують повний список усіх пристроїв/додатків у IACS.

1.4. Висновки щодо посилення систем

Посилення мережевих пристроїв та операційних систем є безперервним процесом, що вимагає постійної уваги.

Суворі процедури

Впроваджувати суворі процедури управління конфігураціями

Регулярний аудит

Регулярно проводити аудит та переглядати налаштування

Ефективне управління патчами

Забезпечувати ефективне управління патчами, включаючи тестування перед розгортанням

1.5. Ключові рекомендації

Обмеження доступу

Обмеження фізичного та логічного доступу є ключовими для зменшення поверхні атаки

Контроль знімних носіїв

Чітка політика щодо використання знімних носіїв є критично важливою

Комплексний підхід

Поєднання всіх заходів безпеки для створення надійної системи захисту

> Успішна реалізація принципів мережевого захисту для ICS/SCADA вимагає системного підходу та постійного вдосконалення процесів безпеки.

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!