Модуль 2. Пристрої та протоколи взаємодії систем ICS/SCADA

Лекція 4: Телекомунікаційні технології в SCADA

Мета лекції

Канали зв'язку

Розглядає канали зв'язку між центром керування та польовими об'єктами, їхні параметри, що впливають на якість та безпеку.

Захист комунікацій

Представляє практичні методи захисту комунікацій: шифрування, VPN, односпрямовані шлюзи даних, сегментацію та контроль трафіку.

Інтернет речей

Аналізує вплив IoT та IIoT на мережеву архітектуру, нові ризики та способи керування ними.

4.1. Дротовий та бездротовий зв'язок для диспетчеризації

4.1.1. Комунікаційна архітектура диспетчерської системи: загальна картина

Ключові компоненти та зв'язки

- Центр керування: Сервери, робочі місця операторів, сховище історичних даних, мережева інфраструктура.
- Польові об'єкти: Контролери, термінальні пристрої, сенсори, виконавчі механізми.
- Транспорт між об'єктами: Провідні та бездротові канали для об'єднання центру керування з віддаленими об'єктами в єдину виробничу мережу.

Критичні параметри зв'язку

- Оцінюйте доступність, затримку (стабільність), пропускну здатність, завадостійкість.
- Забезпечте гарантовану доставку подій та точну синхронізацію часу для коректних журналів, трендів і систем захисту.

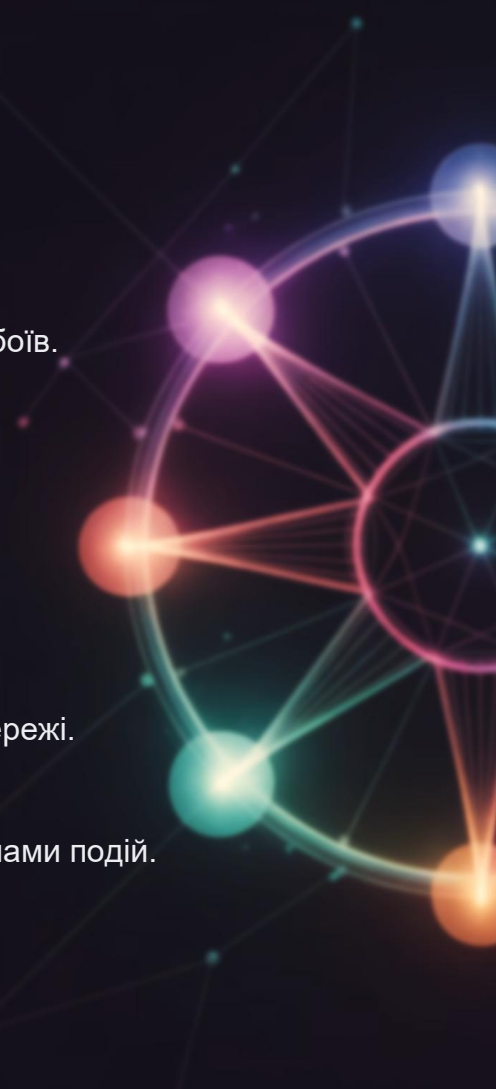
Практичні рекомендації

- Створіть карту зв'язку, що деталізує об'єкти, власників та параметри каналів.
- Визначте мінімальні затримки, допустимі для технологічних процесів, і перевіряйте їх під час приймання мережі.

4.1.2. Локальна мережа в центрі керування

Топології та надійність

- Використовуйте топології: зірка, подвійна зірка, кільце.
- Резервуйте комутатори, дублюйте лінії та незалежні джерела живлення.
- Застосовуйте механізми уникнення мережевих петель та швидкого відновлення після збоїв.
- Об'єднуйте канали (агрегація лінків) для збільшення пропускної здатності та стійкості.



Логічна ізоляція

- Використовуйте віртуальні сегменти (VLAN) для розділення трафіку:
  - Операторські панелі
  - Сховище історичних даних (історик)
  - Інженерні станції
  - Периферійні пристрої
- Налаштуйте маршрутизацію так, щоб виробничий трафік був ізольований від офісної мережі.

Якість обслуговування (QoS)

- Пріоритизуйте телеметрію та команди керування над резервним копіюванням та журналами подій.
- Забезпечте єдиний час у мережі:
  - Використовуйте точний протокол синхронізації (наприклад, NTP).
  - Майте резервне джерело часу.
  - Контролюйте відхилення часу.

4.1.3. Промислові комутатори та фізичне середовище

Вимоги до обладнання

- Захист від пилу, вологи, вібрацій, температур.
- Електромагнітна сумісність.
- Резервне живлення, захист від перенапруг.
- Промислові роз'єми та захищені шафи.

Керування трафіком

- Керуйте багатоадресним трафіком, щоб уникнути перевантажень.
- Фільтруйте надмірний трафік.
- Обмежуйте швидкість та використовуйте черги для "балакучих" пристроїв.

Практичні поради

- Розділяйте кабелі живлення та зв'язку.
- Дотримуйтесь радіусів згину оптоволокна.
- Документуйте всі порти та підключення.
- Передбачте швидку заміну комутатора з відновленням конфігурації.

4.1.4. Послідовні інтерфейси і термінальні сервери

Застосування

- Старі контролери та вимірювальні пристрої з послідовними шинами.
- Довгі шини на базі витої пари.
- Прості віддалені вузли.

Інтеграція в мережу

- Термінальні сервери перетворюють послідовні протоколи на мережеві пакети.
- Конвертери буферизують дані та контролюють тайм-аути/повтори для стабільної роботи на повільних лініях.

Ризики

- Необліковані конвертери створюють загрози безпеці.
- Необхідні зонування, фільтрація портів та облік прошивок кожного перетворювача.

4.1.5. Глобальні мережі між майданчиками

Еволюція та варіанти

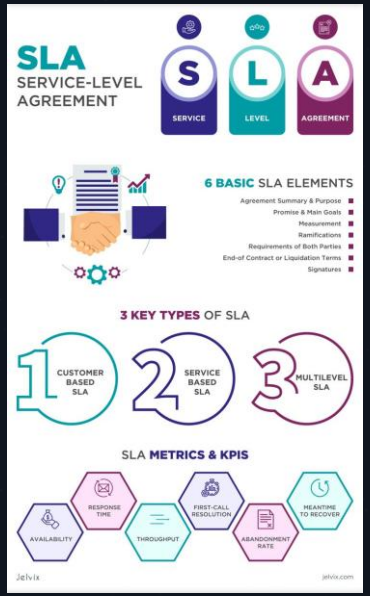
- Перехід від старих комутованих/орендованих ліній до сучасних рішень.
- Використовують приватні мережі провайдерів (MPLS, SD-WAN) або власні оптоволоконні кільця.
- Ці мережі мають суворі угоди про рівень послуг (SLA).

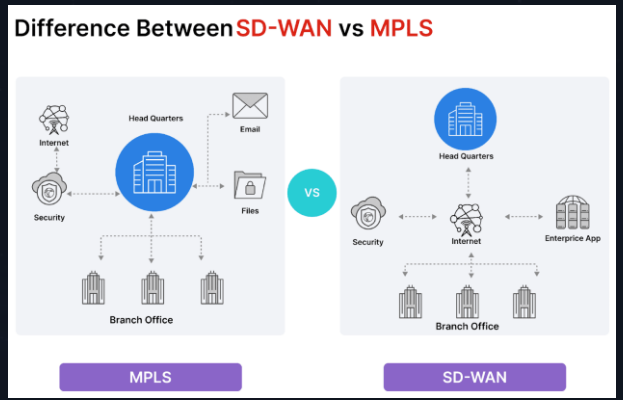
Надійність і затримка

- Застосовуйте кільцеві маршрути з автоматичним перемиканням у разі аварії.
- Постійно перевіряйте стан каналів.
- Розділяйте технологічний та службовий трафік, використовуйте окремі канали для критичних команд.

Проєктні рекомендації

- Забезпечте дві незалежні траси до будівлі з різними точками входу (уникайте єдиного кабелю).
- Регулярно вимірюйте затримки та джитер для кожного напрямку.





4.1.6. Оптоволокно та кільцеві архітектури

01

Технічні переваги

- Низькі втрати та стійкість до електричних перешкод.
- Передача сигналу на великі відстані без підсилення.
- Масштабування пропускної здатності без додаткових кабелів (мультиплексування довжин хвиль).

02

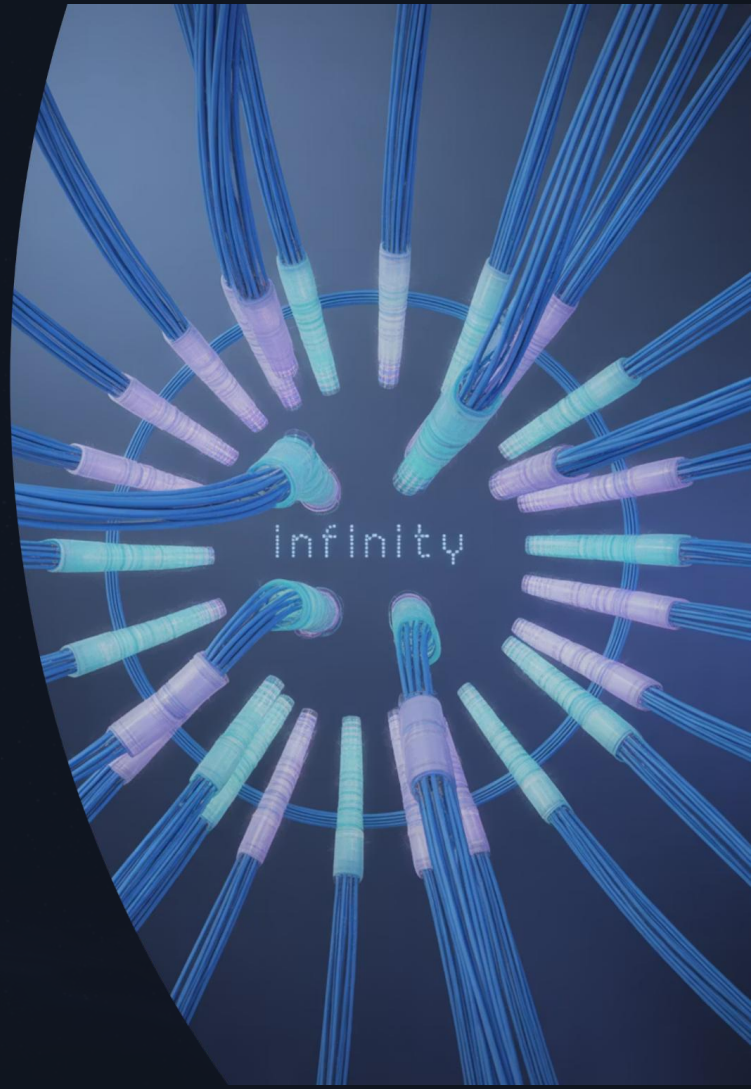
Забезпечення надлишковості

- Кільцеві схеми автоматично перемикають трафік при обриві.
- Контроль часу відновлення для швидкої реакції.
- Використання подвійних кілець (ядро–доступ) для критичних потоків.

03

Експлуатаційні вимоги

- Регулярно перевіряйте чистоту конекторів.
- Ведіть журнал оглядів.
- Забезпечте запас патч-кордів.
- Маркуйте кожну оптичну нитку та крос.



4.1.7. Радіорелейний і мікрохвильовий зв'язок

Сфери застосування

- Далекі відстані
- Складний рельєф
- Швидке розгортання
- Резервування оптоволокна

Планування

- Забезпечте пряму видимість між антенами.
- Розрахуйте запас сигналу з урахуванням згасання.
- Оберіть оптимальний частотний діапазон та ширину каналу.
- Встановіть антени з підігрівом та блискавкозахистом.
- Виконайте вимоги до заземлення щогл.
- Контролюйте погодні ризики.

Безпека

- Використовуйте шифрування на радіоканалі.
- Налаштуйте взаємну перевірку обладнання.
- Фільтруйте службові інтерфейси.

4.1.8. Стільникові мережі для диспетчеризації

Сценарії використання

- Підключення віддалених об'єктів
- Тимчасові рішення
- Резервне копіювання зв'язку

Технічні вимоги

- Окремий профіль доступу оператора для ізоляції трафіку
- Статична IP-адресація
- Білий список пристроїв
- Контроль геозони ввімкнення

Оптимізація радіочастот

- Правильний монтаж антен
- Узгодження параметрів обладнання
- Вимірювання рівня сигналу
- Аудит покриття оператора

4.1.9. Супутниковий зв'язок у віддалених районах

Коли використовувати

Для ізольованих об'єктів без наземної інфраструктури (пустелі, тундра, море).

Ключові аспекти

- Вибір системи: геостаціонарні (вища затримка) або низькоорбітальні (нижча затримка, динамічний трекінг).
- Висока вартість даних: оптимізуйте протоколювання та стискайте дані.

Захист і надійність

- Надійно фіксуйте напрямні антени.
- Забезпечте стійкість до вітрових навантажень та обмерзання.
- Передбачте резервне живлення.

4.1.10. Бездротові локальні технології для диспетчеризації

1

Присутність

Вбудовані в ноутбуки та операторські станції.

2

Правила використання

- Відключення: Вимикайте або фізично видаляйте, де це можливо.
- Доступ: Обмежуйте дозволені точки, використовуйте корпоративну аутентифікацію.
- Ізоляція: Розділяйте бездротових клієнтів та службові мережі.

3

Моніторинг ефіру

- Використовуйте сканери радіоканалу та системи виявлення вторгнень.
- Аналізуйте журнали успішних та невдалих підключень.

4.2. Захист комунікацій: Шифрування, VPN та односпрямовані шлюзи

4.2.1. Криптографічний захист і віртуальні приватні мережі

Що захищаємо:

Ми забезпечуємо конфіденційність та цілісність даних, взаємну перевірку сторін, а також захист від підміни та прослуховування.

Керування ключами:

Для ефективного керування ключами застосовуємо:

- Власну інфраструктуру відкритих ключів (PKI).
- Чітко визначені терміни дії сертифікатів.
- План ротації ключів.
- Списки відкликаних сертифікатів.
- Апаратні сховища ключів.

Використовувані інструменти:

- Протоколи захищених сесій: для веб-доступу, диспетчерських шлюзів та сучасних серверів промислових даних.
- Мережева криптографія (VPN): для шифрування тунелів між об'єктами та забезпечення віддаленого доступу інженерів.

Практичні рекомендації:

- Обов'язково шифруйте всі міжмайданчикові канали.
- Розділяйте ролі: експлуатація мережі та видача сертифікатів мають бути незалежними.

4.2.2. Периметри, сегментація і фільтрація трафіку

Архітектурні принципи

- Розділяйте виробничу мережу на зони безпеки.
- Обмінюйтеся даними між зонами лише через контрольовані канали.
- Використовуйте проміжну (буферну) зону між виробничою та корпоративною мережами для безпечного обміну, запобігаючи прямому доступу.

Контроль трафіку

- Встановлюйте міжмережеві екрани, що аналізують промислові протоколи.
- Обмежуйте команди за функціональними кодами, частотою запитів і напрямком.
- Застосовуйте принцип «заборонити все, що не дозволено» для мереж і портів.

Моніторинг

- Використовуйте дзеркальні порти на комутаторах.
- Застосовуйте колектори потоків і системи аналітики.
- Шукайте аномалії в промисловому трафіку для підвищення безпеки.

4.2.3. Односпрямовані передавачі даних і симплексні потоки

Принцип дії

Дані передаються лише в один бік: з виробничої мережі до менш довірених сегментів. Зворотний потік фізично неможливий (на рівні світла або електроніки).

Сфери використання

- Передача телеметрії, журналів та даних безпеки до аналітичних платформ.
- Реплікація історичних даних без можливості зовнішнього управління.

Особливості впровадження

- Налаштуйте прикладні шлюзи, які емулюють підтвердження для сумісності.
- Проведіть ретельне тестування схем обміну даними.
- Використовуйте криптомодеми з апаратним шифруванням для послідовних ліній.

4.2.4. Віддалене обслуговування і контроль доступу

Організаційні заходи

- Використання перехідних серверів із записом сесій.
- Двофакторна автентифікація.
- Обмежений за часом доступ.
- Схвалення всіх заявок на доступ.
- Тимчасові облікові записи з автовимкненням.
- Розділення прав: "тільки читання" та "керування".

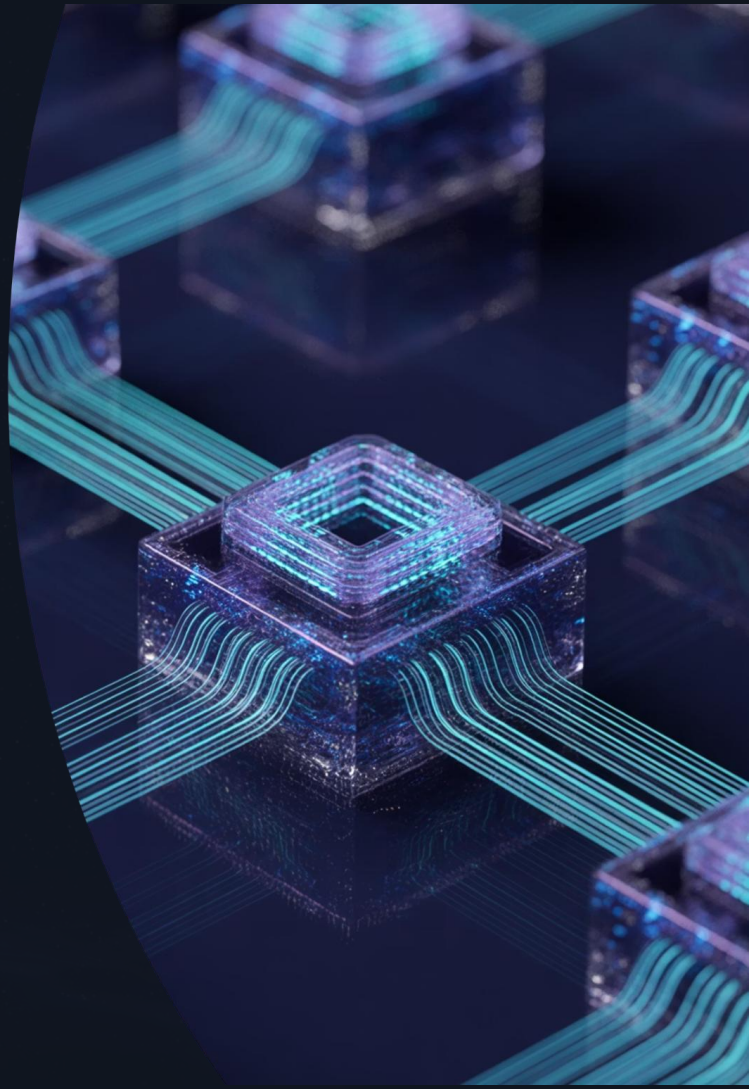
Технічні обмеження

- Заборона одночасного підключення ПК до виробничої та корпоративної мереж.
- Окремі інженерні ноутбуки:
  - З контрольованим ПЗ.
  - З перевіркою зовнішніх носіїв.
  - З журналюванням підключень.

Моніторинг

- Аналіз дій користувачів та мережевих подій.
- Сповіщення про зміни в логіці контролерів.
- Резервний канал для швидкого блокування доступу.

4.3. Як IoT та IIoT змінюють комунікації



4.3.1. Шлюзи, брокери повідомлень та хмарні інтеграції

Шлюзи

- Перетворюють промислові протоколи на потік подій.
- Буферують дані та знижують навантаження на мережу.
- Виконують локальну аналітику на місці.

Брокери повідомлень

- Використовують модель публікації-підписки для взаємодії сенсорів і сервісів.
- Забезпечують безпеку через захищені з'єднання, перевірку сертифікатів, авторизацію доступу та обмеження керуючих каналів.

Хмарні патерни

- Ініціюють вихідні з'єднання з проміжної зони, щоб уникнути відкриття вхідних портів до виробничих мереж.
- Забезпечують односторонню реплікацію даних у хмару, зберігаючи локальні копії.

4.3.2. Ідентичність пристроїв, керування прошивками та життєвим циклом

Ідентичність і довіра

- Використовуйте унікальні сертифікати пристроїв, відмовтеся від стандартних паролів.
- Фіксуйте інвентарні дані та прив'язуйте пристрої до мережевих сегментів.
- Ведіть журнали змін конфігурації.
- Отримуйте сповіщення про підміну або додавання невідомих вузлів.

Оновлення і відкат

- Забезпечте захищені бездротові оновлення (OTA) з цифровим підписом.
- Запровадьте поетапне розгортання оновлень.
- Перевіряйте сумісність оновлень з технологічними процесами.
- Передбачте можливість швидкого відкату до попередньої версії.
- Визначте планові вікна для оновлень.
- Використовуйте тестові полігони.
- Застосовуйте обов'язкові чек-листи приймання.

Масштаб і моніторинг

- Впровадьте автоматизовані системи керування конфігураціями.
- Групуйте пристрої за зонами та рівнем критичності.
- Збирайте метрики стану та безпеки для кожного класу пристроїв.

4.4. Підсумки і практичні орієнтири

Ключові висновки

- Диспетчерські системи використовують багато каналів зв'язку. Кожен має свої ризики, тому потрібна надійна архітектура безпеки.
- Для захисту комунікацій застосовуйте шифрування, сегментацію, контрольований віддалений доступ, моніторинг та, за потреби, односпрямовані шлюзи.
- Промисловий Інтернет речей (IIoT) розширює мережевий периметр. Це вимагає суворого керування ідентичністю, оновленнями та брокерною архітектурою з чіткими правилами.

Практичні кроки впровадження

- Складіть повну карту комунікаційних каналів, визначте відповідальних та їхні параметри.
- Уніфікуйте шифрування та політики VPN; впровадьте інфраструктуру сертифікатів.
- Створіть демілітаризовану зону (ДМЗ) між виробничою та корпоративною мережами; використовуйте брандмауери з аналізом промислових протоколів.
- Окремо регулюйте використання мобільного, бездротового та супутникового доступу, включно з вимогами до обладнання та журналювання.
- Для інтеграції IIoT впровадьте унікальну ідентичність пристроїв, захищені брокери, контроль обміну даними та планові оновлення прошивок.

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!