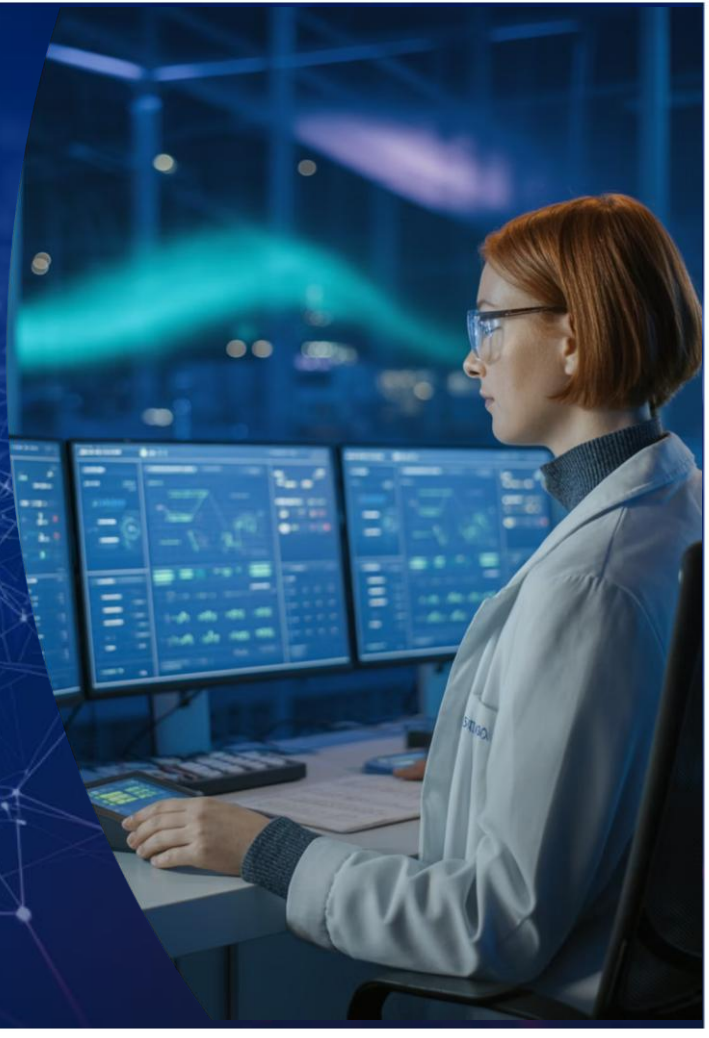
Модуль 2. Пристрої та протоколи взаємодії систем ICS/SCADA

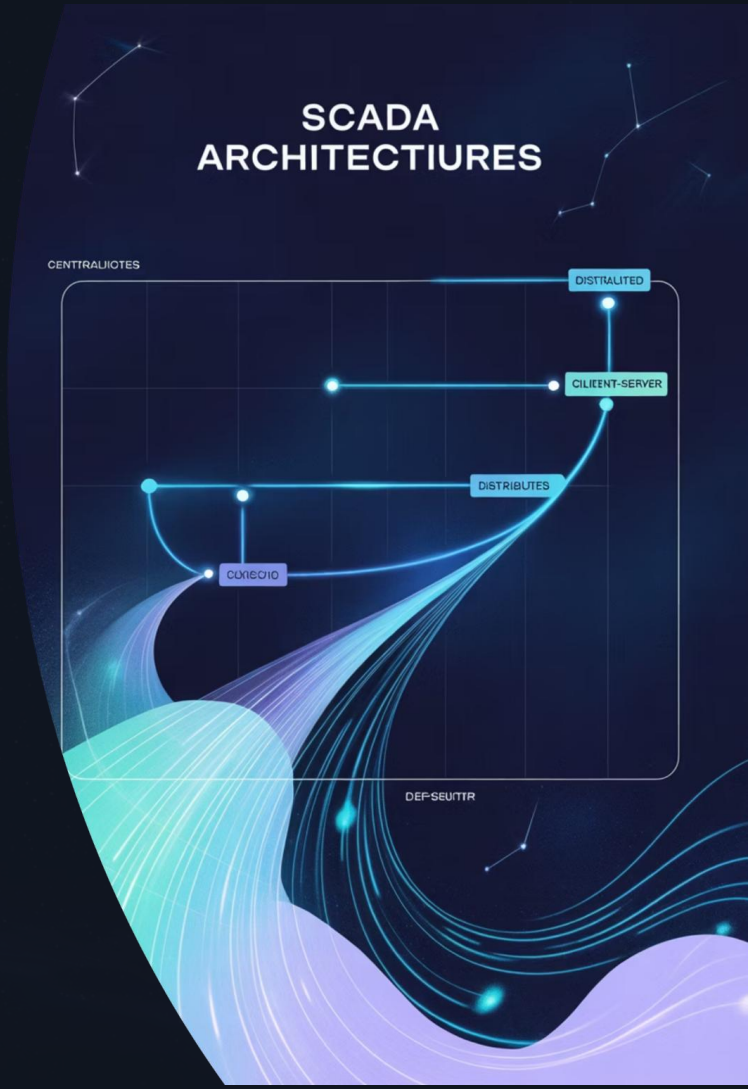
Лекція 2: Архітектури систем SCADA та їх еволюція



Мета лекції

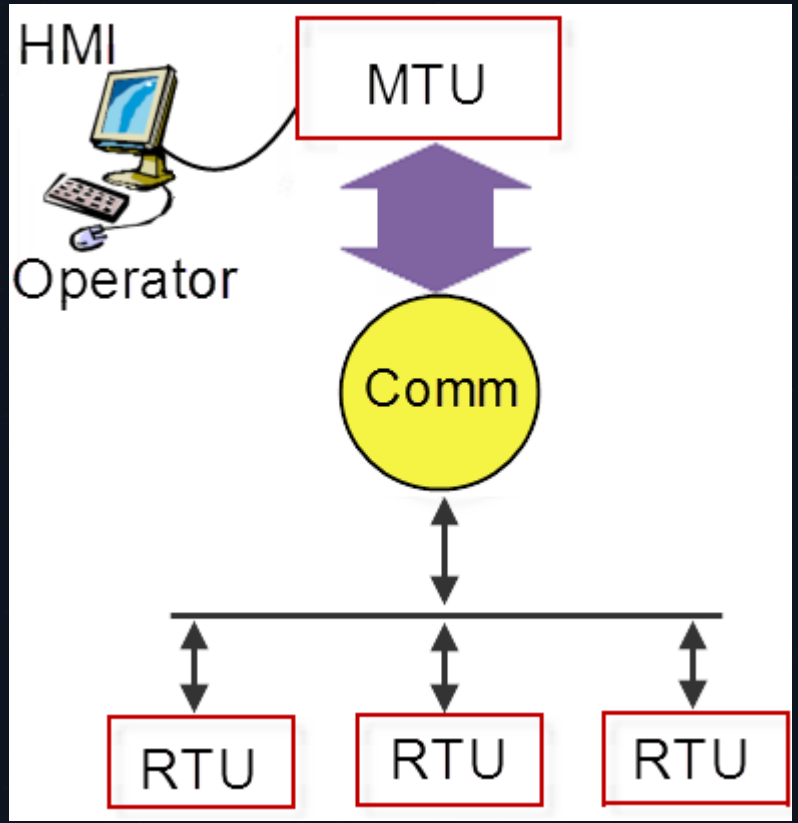
- [ ] Показати еволюцію від централізованих до розподілених і клієнт-серверних SCADA
- [ ] Пояснити перехід від пропрієтарних платформ до COTS та наслідки для безпеки
- [ ] Розкрити, як віртуалізація змінює проєктування, експлуатацію і кіберзахист SCADA

2.1. Централізовані, розподілені та клієнт-серверні архітектури



2.1.1. Централізовані SCADA перших поколінь

- Перші системи диспетчерського керування з'явилися у 1960-х на мейнфреймах. Термін SCADA утвердився у 1980-х.
- Вся логіка і збір даних зосереджувались на одному центральному вузлі MTU Master Terminal Unit, тобто головному термінальному блоці.
- Польові майданчики оснащувались RTU Remote Terminal Unit, тобто віддаленими терміналами, що читали датчики та керували актуаторами.
- Операції були переважно опитувальними читання аналогових і дискретних сигналів, фіксація тривог, видача простих команд у каналах низької пропускної здатності.



2.1.2. Потоки даних і інтерфейси централізованої архітектури

1

HMI

HMI Human Machine Interface, людино-машинний інтерфейс працював у центрі керування та відображав дані, які подавав MTU.

2

Лінії зв'язку

Лінії зв'язку використовували тональну телеметрію, виділені пари, радіоканали, пізніше комутовані лінії.

3

Цикл опитування

Типовий цикл опитування будувався як послідовне звернення MTU до кожного RTU з жорсткими тайм-аутами. Пропуск кадру означав втрату оновлення до наступного кола.

Єдина точка відмови у MTU і в магістральному каналі створювала ризик загального простою.

2.1.3. Експлуатаційні обмеження централізованих рішень

Обмежена масштабованість

кількість RTU і довжина циклу опитування ростуть швидше, ніж ресурси одного MTU.

Надійність

залежить від одного сервера і одного сегмента зв'язку.

Обмежені механізми пріоритезації

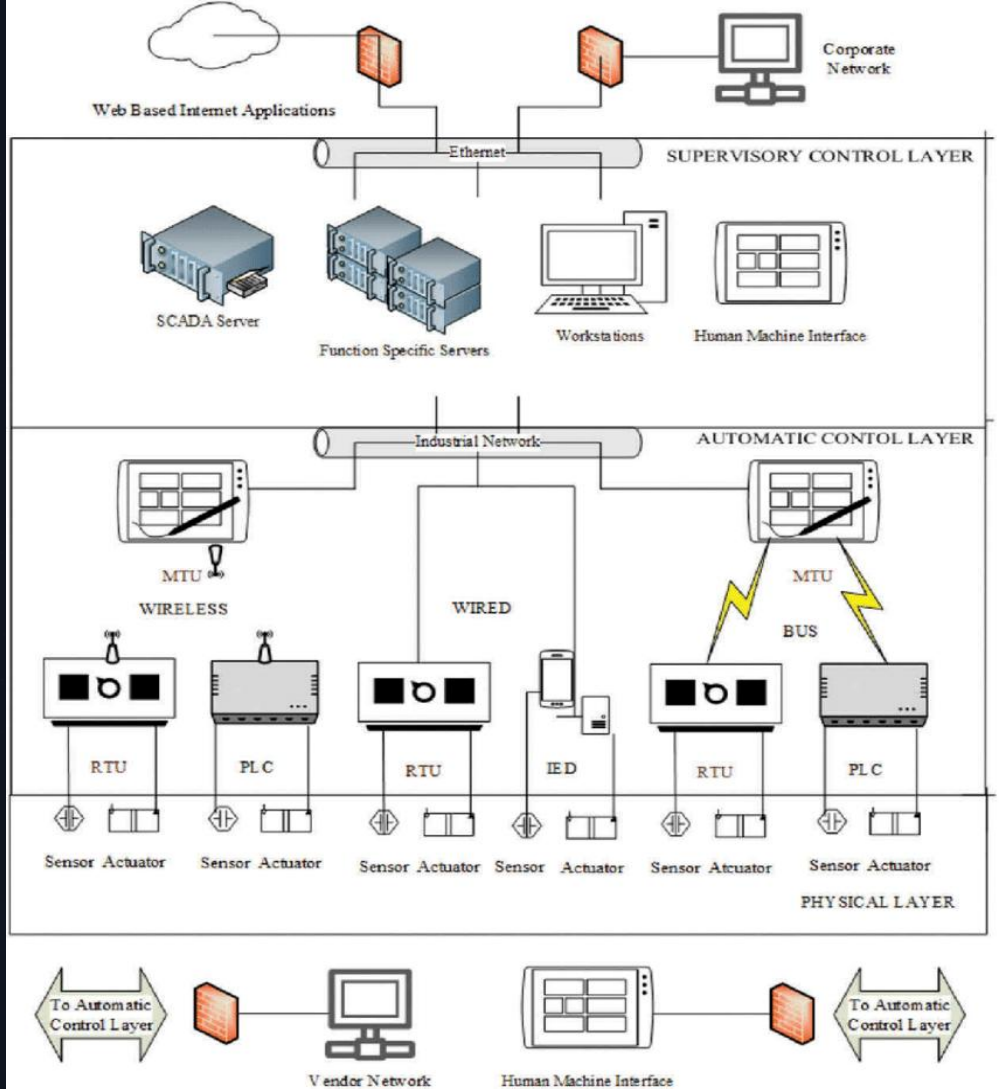
тривог порівняно з потоками трендів та службовими повідомленнями.

Ручні процедури

перемикання і відсутність тонкої телеметрії ускладнювали діагностику інцидентів.

2.1.4. Перехід до розподілених архітектур

- Збільшення кількості RTU змусило розкладати навантаження на регіональні вузли sub-MTU, що агрегують дані й події.
- З'явились резервні та регіональні центри керування для підвищення стійкості і зменшення затримок.
- Попередню обробку подій перенесли ближче до поля для економії трафіку магістралей та швидкої локальної реакції.
- Упровадили дублювання каналів і автоматичне прийняття резервних ролей при відмові.



2.1.5. Топології розподіленого зв'язку

Точка-точка і «серія»

придатні для невеликих ліній, але мають кумулятивні затримки та крихкість у разі відмови проміжного вузла.

«Зірка» і «серія-зірка»

централізують комутацію і спрощують локалізацію аварій.

Кільця з відновленням

на канальному рівні скорочують час конвергенції після обривів.

Мультикаст подій

передає тільки зміни станів замість суцільного опитування, що радикально економить канал.

2.1.6. Клієнт-серверна модель у сучасній SCADA

Поява мікропроцесорних серверів, мереж TCP/IP Transmission Control Protocol over Internet Protocol і швидкісних LAN Local Area Network пришвидшила перехід до сервісної декомпозиції.

Вузли HMI, інженерні станції та історики працюють як клієнти, які підписуються на сервіси реального часу, тривог і архівів центральних SCADA-серверів.

Ролі розносять на окремі сервери реальний-час, тривоги, архів, звіти з власним масштабуванням і відмовостійкістю.

Для обміну між центрами енергетики використовується ICCP Inter-Control Center Communications Protocol, що також дотримується моделі клієнт-сервер.

2.1.7. Продуктивність і керованість клієнт-серверної SCADA

01

Черги повідомлень і кеші

Впроваджуються черги повідомлень і кеші, щоб вирівнювати пікові навантаження і не перевантажувати HMI оновленнями.

02

Якість обслуговування

Налаштовується якість обслуговування щоб тривоги і команди мали пріоритет над трендовими потоками.

03

VLAN сегментація

Логічно відокремлюються домени у VLAN Virtual LAN, віртуальних локальних мережах для HMI, інженерії, істориків, шлюзів у WAN Wide Area Network.

04

Керування доступом

Запроваджується керування доступом за ролями і наскрізне журналювання дій операторів та інженерів.

2.2. Еволюція від пропрієтарного до COTS

2.2.1. Від пропрієтарних платформ до COTS

1

Пропрієтарні системи

Ранні SCADA ґрунтувалися на унікальному апаратному забезпеченні і власному ПЗ, що замикало замовника на одного вендора.

2

Масовий ринок

Масовий ринок серверів і операційних систем знизив вартість та прискорив модернізації.

3

COTS переваги

COTS Commercial Off-The-Shelf приніс сумісність з типовими інструментами резервування, бекапів і моніторингу, а також кращу керованість ресурсами.

Функції вендорів змістилися у бік платформ, ліцензій і сервісів, тоді як базові ОС, мережі та «залізо» обслуговують IT-підрозділи підприємств.

2.2.2. Типовий технологічний стек на COTS

Сервери x86

під керуванням Windows або Linux з кластеризацією та апаратною віртуалізацією.

Сховища і СКБД

для історіків від класичних реляційних до time-series.

Мережі Ethernet

і TCP/IP для транспорту, промисловий Ethernet у полі.

Інтеграція

через API Application Programming Interface та OPC OLE for Process Control з переходом на OPC UA Unified Architecture з вбудованою автентифікацією і шифруванням.

2.2.3. Наслідки COTS для кібербезпеки

⚠ Основні ризики COTS

- Спільні ОС і СКБД у IT та OT означають спільні вразливості і повторювані техніки атак.
- Публічна інформація про експлойти спрощує підготовку зловмисників до атак на SCADA, що використовують стандартні компоненти.
- Зростає поверхня атаки через типові служби за замовчуванням і відомі порти.

> Висновок безпеку вбудовують у архітектуру, процеси конфігурації, керування патчами та моніторинг, а не покладаються на «секретність» реалізації.

2.2.4. Керування змінами і патчами у середовищі COTS

1

Реєстр активів

Повний реєстр активів версії ОС, бібліотек, драйверів і залежностей, матриця критичності та власники.

2

Тестові полігони

Тестові полігони, що відтворюють виробничі навантаження, для перевірки патчів і змін конфігурацій.

3

Планові вікна

Планові вікна обслуговування з чітким сценарієм відкату, перевірками після змін і комунікаціями з виробництвом.

4

«Загартування» хостів

«Загартування» хостів вимкнення зайвих служб, мінімальні ролі, білі списки застосунків, контроль переносних носіїв.

2.2.5. OPC і відкриті інтерфейси

Еволюція OPC

- OPC Classic на DCOM у межах Windows ускладнював роботу через міжмережеві екрани і NAT.
- OPC UA привніс платформну незалежність, модель інформації, сесії з сертифікатами і шифруванням трафіку.

Сучасні API

- Вендорні API REST або gRPC спрощують інтеграцію з аналітикою і мобільними клієнтами, але потребують керування ключами і версіями.
- Необхідні процеси керування сертифікатами, ротація ключів і політики доступу для машинних облікових записів.

2.3. Віртуалізація в системах SCADA

2.3.1. Концепція віртуалізації у SCADA

Віртуальна машина

Віртуальна машина VM Virtual Machine це ізольований екземпляр ОС і застосунків на спільному фізичному сервері.

Гіпервізор

Гіпервізор керує розподілом ресурсів між VM, буває типу bare-metal із прямим доступом до апаратури або hosted поверх наявної ОС.

Переваги віртуалізації

Віртуалізація дозволяє консолідувати сервери, прискорити розгортання, робити знімки стану та клонувати середовища для тестування.

SCADA на VM

У SCADA це означає запуск ролей реального часу, тривог і історіків на відокремлених VM із платформою високої доступності.

2.3.2. Патерни розгортання віртуалізованої SCADA

Кластери у центрі обробки даних

підприємства забезпечують відмовостійкість критичних сервісів із гарячим перемиканням.

Edge-вузли

близько до технологічного процесу тримають локальні кеші даних і автономні сценарії на випадок обриву зв'язку.

Рознесення ролей

на окремі VM для ізоляції навантажень реальний-час, історики, інженерні станції, шлюзи у зовнішні мережі.

Спільні сховища

на LUN і віртуальні комутатори з окремими сегментами трафіку керування, даних і резервного копіювання.

2.3.3. Час і продуктивність у VM

Синхронізація часу

Синхронізація часу критична для коректних штампів тривог і трендів використовують NTP Network Time Protocol або PTP Precision Time Protocol для вищої точності.

Закріплення ядер

Закріплення ядер процесора за критичними VM зменшує джиттер і робить затримки прогнозованими.

Пряме проходження

Пряме проходження вводу-виводу через SR-IOV або PCIe-passthrough знижує накладні витрати мережевих і дискових операцій.

Контроль затримок

Постійний контроль затримок і втрат пакетів у каналах реального часу з порогами та оповіщеннями.

2.3.4. Безпека, резервування і відновлення у віртуальному світі

Гіпервізор як корінь довіри Гіпервізор стає коренем довіри його мінімізують, адміністрування відокремлюють, доступ захищають багатофакторною автентифікацією.	**Ізоляція мереж VM** Мережі VM ізолюють політиками у VLAN та окремими vSwitch, керувальні інтерфейси винесені у відокремлені сегменти.
Цілісність образів Образи VM підписуються, цілісність перевіряється, конфігурації зберігаються як код для відтворюваності і аудиту.	**Резервне копіювання** Резервне копіювання поєднує повні та інкрементальні бекапи, журналювання транзакцій історіків і геореплікацію. Визначаються показники RTO час відновлення та RPO втрата даних. Регулярно тренуються сценарії перемикання.

2.4. Підсумкові висновки

Еволюція архітектури

Еволюція від монолітних централізованих рішень до розподілених і сервісних моделей дала масштабованість і стійкість, але підвищила складність і вимоги до процесів.

Віртуалізація

Віртуалізація стала стандартом для ролей SCADA, проте вимагає уваги до гіпервізора, ізоляції мереж і детермінізму часу.

Вплив COTS

Використання COTS зблизило OT з IT та принесло типові кіберризики, які компенсують архітектурою, конфігураційною дисципліною і моніторингом.

Кіберстійкість

Кіберстійкість SCADA спирається на три стовпи архітектуру, дисципліну експлуатації та безперервний моніторинг зі швидким відновленням.

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!