Модуль 2. Пристрої та протоколи взаємодії систем ICS/SCADA

Лекція 3: Протоколи промислових систем керування

Мета лекції

Цілісна картина

Дати цілісну картину промислових протоколів у середовищах ICS та SCADA.

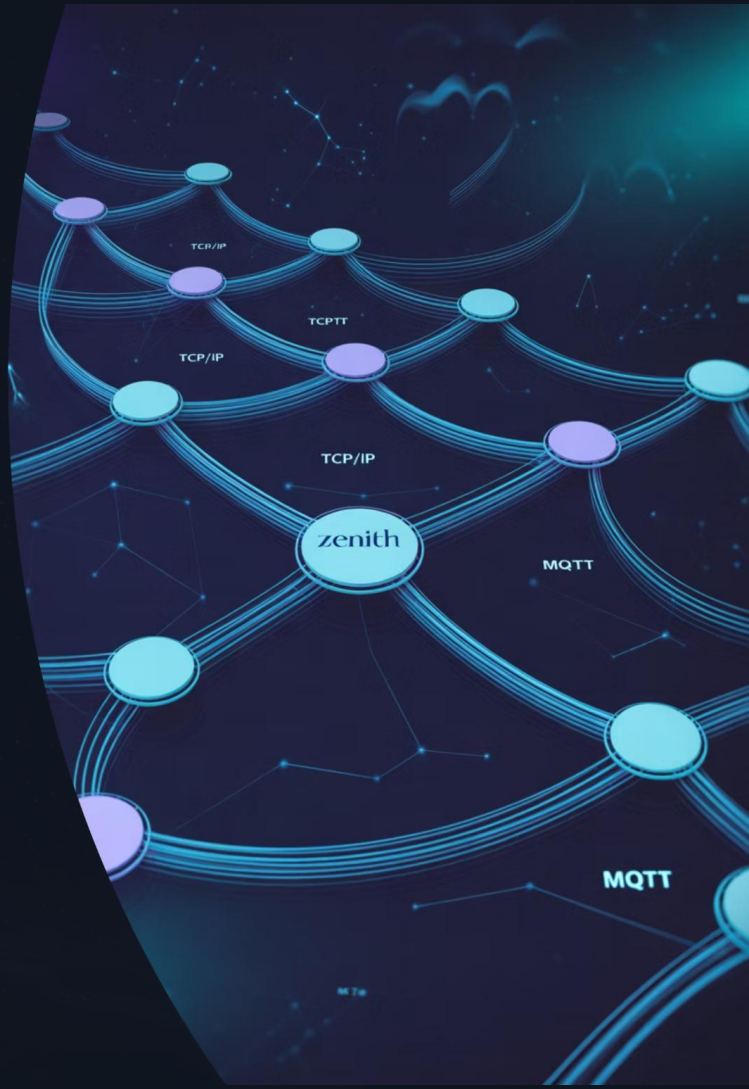
Аналіз протоколів

Пояснити сильні та слабкі сторони конкретних протоколів і їх наслідки для безпеки.

Практичні навички

Показати практики пасивного аналізу трафіку для виявлення загроз і побудови реєстру активів.

3.1. Огляд і класи промислових протоколів



3.1.1. Класи взаємодії

Контролер ↔ польовий пристрій

Modbus, DNP3, IEC 60870-5-101, EtherNet/IP, PROFINET, EtherCAT.

Контролер ↔ контролер

S7, IEC 60870-5-104, IEC 61850, CIP.

Сервер даних ↔ клієнти

HMI, історики OPC Classic, OPC UA.

Центр ↔ центр

ICCP TASE.2 для міжсистемного обміну в енергетиці.

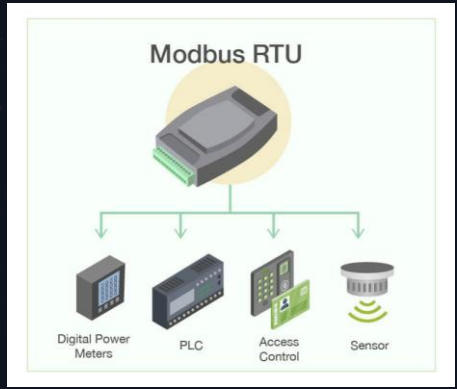
Транспорт і фізика

- Серіальні канали RS-232, RS-485 для Modbus-RTU, DNP3-Serial.
- IP-мережі Ethernet, TCP/IP Transmission Control Protocol over Internet Protocol, UDP User Datagram Protocol.
- Промисловий Ethernet і специфічні часові механізми реального часу.

3.1.2. Modbus як найпоширеніший протокол польового рівня

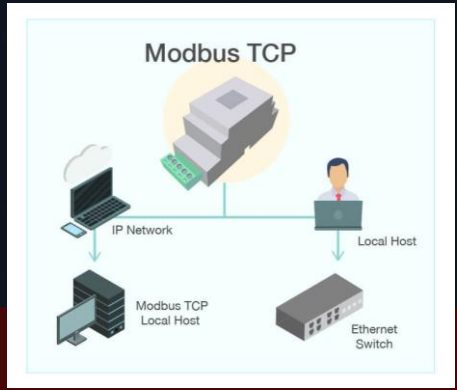
Що це таке

- Modbus відкритий прикладний протокол обміну між контролерами і пристроями вводу-виводу.
- Реалізації Modbus-RTU серіальний режим і Modbus/TCP поверх TCP порт 502.



Адресність і моделі даних

- Coils бітові виходи, Discrete Inputs бітові входи, Holding Registers 4xxxx, Input Registers 3xxxx.
- Функціональні коди читання 01, 02, 03, 04 і запис 05, 06, 15, 16.
- Типова телеметрія рівнів, тиску, станів, а також дистанційні команди.



Обмеження безпеки

- Немає автентифікації та шифрування, відсутній контроль цілісності на рівні протоколу.
- Легке підроблення відповіді, перехоплення і повтор команд replay, несанкціонований запис регістрів.

3.1.3. Практичні аспекти Modbus у мережі

Топові ризики

- Відкритий порт 502 на маршрутизованих сегментах і в DMZ Demilitarized Zone призводить до широкої видимості.
- Відсутність ролей і прав на рівні протоколу.
- Уразливість до сканування та інвентаризації пристроїв за сигнатурою банера.

Компенсуючі заходи

- Сегментація зон і трактів за ISA/IEC 62443, фільтрація лише необхідних функціональних кодів і адрес.
- Проксі-шлюзи з Deep Packet Inspection глибинний аналіз пакетів для Modbus і білоспискові політики.
- Тунелювання поверх TLS Transport Layer Security або IPsec за межами технологічної мережі.

3.1.4. Протокольна сім'я Siemens S7

Що це таке

S7/S7comm та S7commPlus пропрієтарні протоколи Siemens для PLC SIMATIC S7 програмування, діагностика, обмін даними.

Використання на канальному рівні Ethernet з власною інкапсуляцією або TCP.

Особливості

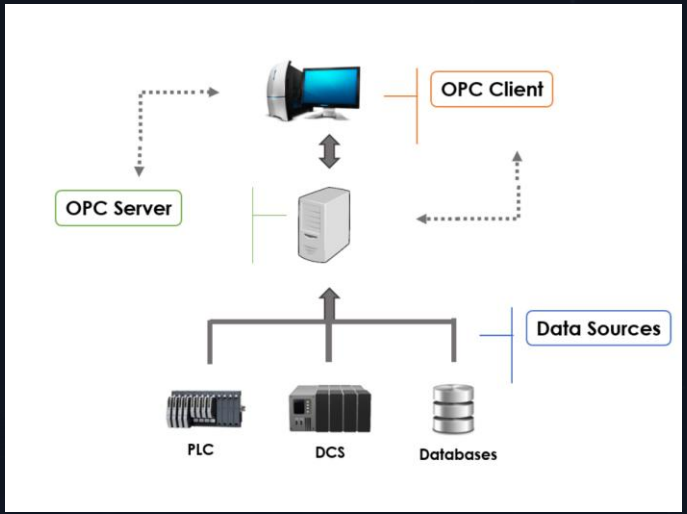
Багато команд керування пам'яттю PLC, завантаження логіки, читання тегів.

Історично без криптозахисту та з обмеженими механізмами авторизації на рівні протоколу старі покоління.

Покращення безпеки

Новіші прошивки з'явилися з TLS-каналами, сертифікатами та рольовою моделлю, але потребують правильного налаштування і оновлень.

3.1.5. OPC Classic як універсальна шина даних Windows



Що це таке

OPC OLE for Process Control стандарт клієнт-серверного обміну даними між HMI, історіками і драйверами до PLC.

Працює поверх DCOM Distributed Component Object Model у Windows.

Сильні сторони

- Багаті моделі даних, події та тривоги, часові мітки і якість.
- Широка підтримка в інструментах візуалізації.

Слабкі місця

- DCOM складний у брандмауерах, чутливий до версій і прав доступу.
- Вбудованих сучасних механізмів безпеки обмаль, трафік часто у відкритому вигляді.

3.1.6. OPC UA Unified Architecture як сучасна взаємодія OT↔IT

Архітектура

Платформно незалежний стек, клієнт-сервер і PubSub, модель інформації з типізацією та простором адрес.

Вбудовані механізми шифрування, автентифікації, підписів і управління сесіями.

Переваги

Єдиний канал до різнорідних джерел даних, стандартизовані профілі безпеки.

Підтримка сертифікатів, ролей і політик доступу для користувачів і застосунків.

Застереження

Безпека залежить від життєвого циклу сертифікатів і правильної конфігурації політик.
Необхідні процеси ротації ключів і моніторинг відхилених сесій.

3.1.7. DNP3 для енергетики та інфраструктури води

Що це таке

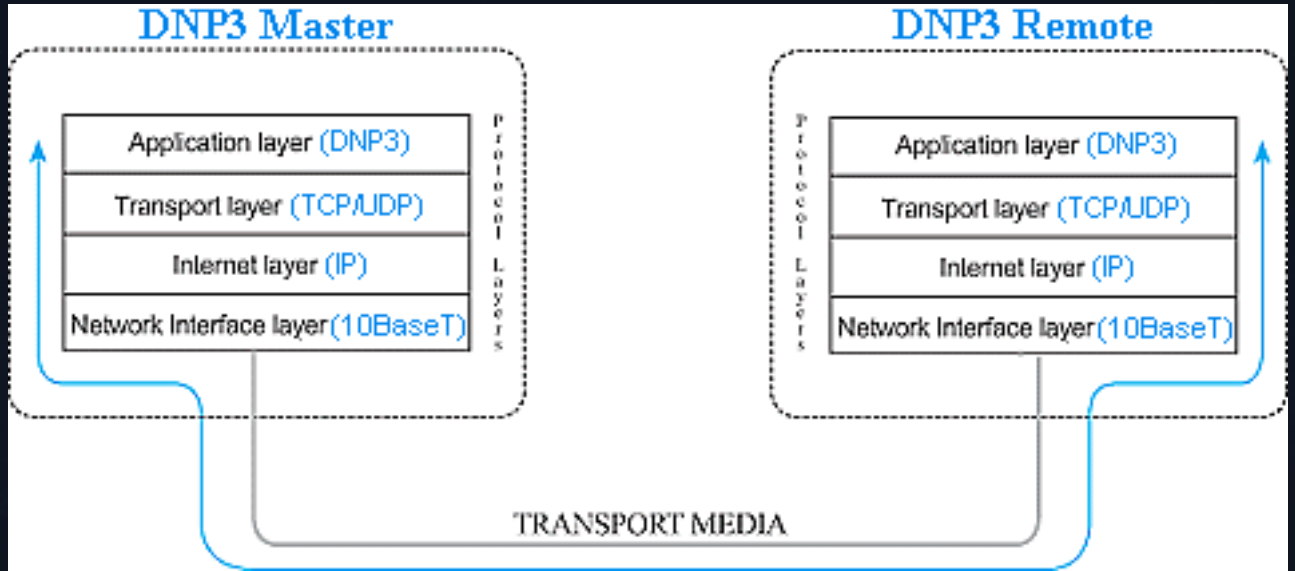
DNP3 Distributed Network Protocol телеметрія між центром і RTU Remote Terminal Unit, IED Intelligent Electronic Device.

Працює серійно або поверх TCP/UDP. Має багатий клас об'єктів, підтвердження, часові позначки.

Безпека

Базовий протокол без криптографії.

Розширення DNP3 Secure Authentication додає автентифікацію команд і подій, але його треба окремо ввімкнути і підтримувати всіма учасниками.



3.1.8. IEC 60870 та ICCP TASE.2 для диспетчерських центрів

1

IEC 60870-5

101 серійний і 104 IP-варіант для телемеханіки підстанцій, широко застосовується в Європі.

Простий транспорт станів і вимірів, події з часовими мітками.

2

ICCP TASE.2 IEC 60870-6

Inter-Control Center Communications Protocol для обміну між диспетчерськими центрами.

Історично покладається на зовнішній захист каналу VPN Virtual Private Network, IPsec або TLS.

ACSE автентифікація додатків існує, але не обов'язкова, що вимагає посиленого мережевого захисту.

3.1.9. EtherNet/IP і стек CIP у дискретному виробництві

Що це таке

EtherNet/IP Ethernet Industrial Protocol реалізація CIP Common Industrial Protocol поверх стандартного Ethernet і TCP/UDP. Широко використовується в приводах, роботах, датчиках.

Мережеві особливості

- Активно застосовує multicast для трафіку реального часу. Потрібен IGMP snooping і querier, інакше мережу заливає потік.
- Контроль пріоритетів і смуг потрібен для стабільної латентності.

> ⚠ **Безпека**
>
> Базовий протокол без вбудованого шифрування, покладається на сегментацію, DPI-шлюзи і захищені тунелі ззовні.

3.1.10. Інші важливі протоколи OT

PROFINET

Промисловий Ethernet з режимами RT та IRT для детермінованих часових вимог.

EtherCAT

«On-the-fly» обробка кадрів із дуже малою затримкою, жорсткі вимоги до топології.

IEC 61850

Енергетика, сервіси MMS Manufacturing Message Specification і телезахист GOOSE Generic Object Oriented Substation Event.

BACnet

Автоматизація будівель, різні транспортні середовища, часто відкриті порти в корпоративних мережах.

MQTT і AMQP

Легковагі брокерні протоколи для IIoT Industrial Internet of Things, потребують TLS і керування ідентичностями.

3.1.11. Порівняння протоколів за ключовими критеріями

Критерій	Опис
Транспорт	серійний чи IP, чи підтримуються обидва режими.
Модель даних	прості регістри і біти проти типізованих об'єктів і подій.
Час реального часу	детермінізм і механізми пріоритетів.
Вбудована безпека	наявність автентифікації, підписів, шифрування.
Розповсюдженість	у галузях енергетика, вода, нафта і газ, дискретне виробництво, будівлі.
Зрілість інструментів	моніторингу і DPI для SOC Security Operations Center.

3.2. Слабкі місця безпеки застарілих протоколів

3.2.1. Історичні припущення, що зробили ОТ-протоколи вразливими

Ізольовані мережі

Проєктувалися для ізольованих мереж і довірених користувачів, без загрози з Інтернету.

Пріоритет доступності

Пріоритет доступності та детермінізму над конфіденційністю і цілісністю.

Мінімалізм повідомлень

Мінімалізм у повідомленнях заради економії каналу відсутність полів для підписів і nonce.

Обмежені ресурси

Вузькі ресурси польових пристроїв, що ускладнювали криптографію.

3.2.2. Типові вектори атак на OT-протоколи

Man-in-the-Middle
підміна показів і команд на незахищених каналах.

Replay
повтор легітимних команд без захисту від відтворення.

Неавторизований запис
регістрів Modbus або завантаження логіки через S7.

Травлення мережі
multicast-штормами EtherNet/IP без IGMP-контролю.

Зловживання службами
автоконфігурації і «заводськими» обліковими записами.

3.2.3. Архітектурні компенсатори для «несек'юрних» протоколів

Сегментація зон

Сегментація зон і трактів за ISA/IEC 62443, мінімальні маршрути між IT і OT.

Технологічні брандмауери

Технологічні брандмауери з DPI для Modbus, DNP3, S7, IEC 104, CIP, GOOSE.

Односторонні шлюзи

Односторонні шлюзи data diode для телеінформації, що не потребує команд назад.

Білі списки

Білі списки функціональних кодів, адрес і частот опитування, виявлення відхилень.

Тунелі VPN

Тунелі VPN з TLS або IPsec на міжсайтових лінках, сертифікатна модель довіри.

3.2.4. Процеси і експлуатаційна дисципліна

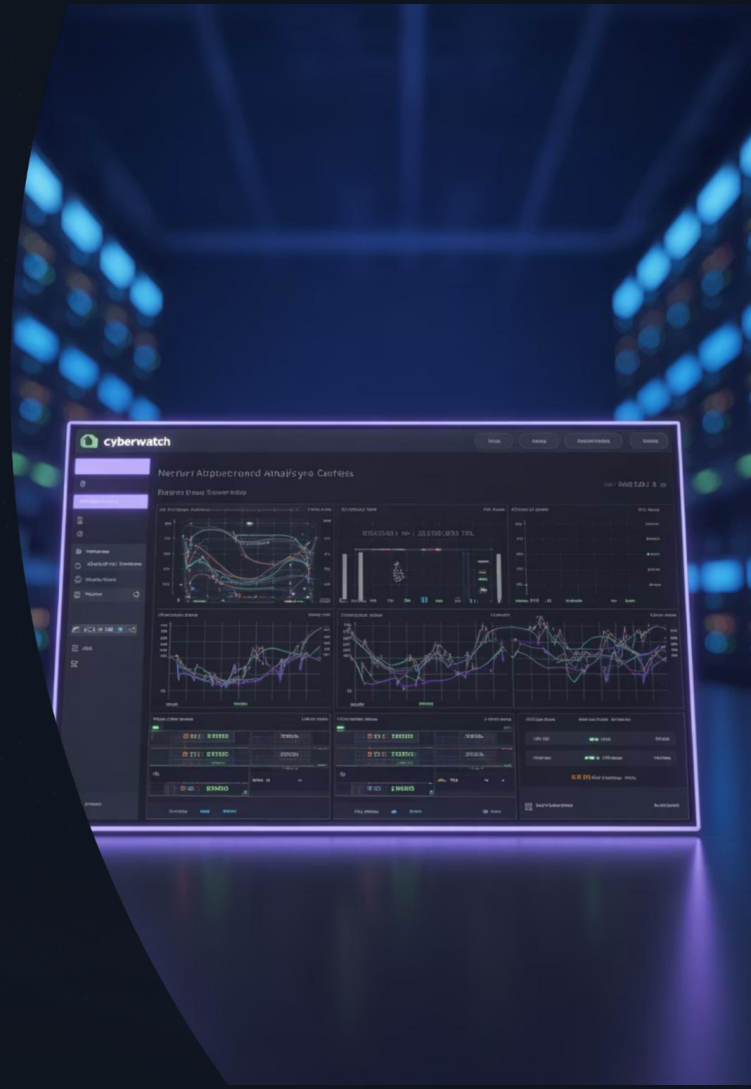
Управління змінами

- Управління змінами і патчами з тестовими полігонами, щоб не зірвати виробництво.
- Жорсткий контроль доступу до інженерних станцій і портативних носіїв.
- Розмежування повноважень між операторами, інженерами і підрядниками.

Моніторинг і аудит

- Журналювання команд і аудит дій із кореляцією в SIEM Security Information and Event Management.
- Безперервний моніторинг трафіку і цільові «сигнали тривоги» на критичні події протоколів.

3.3. Захоплення і перегляд протоколів ICS



3.3.1. Пасивний моніторинг як базова практика в ОТ

Захоплення трафіку

Використання SPAN-портів і мережевих TAP для копій трафіку без впливу на процес.

Розміщення сенсорів

Розміщення сенсорів у ключових точках між зонами, на виходах із трактів, біля шлюзів у WAN Wide Area Network.

Синхронізація часу

Синхронізація часу NTP Network Time Protocol або PTP Precision Time Protocol для коректної реконструкції подій.

Реєстр активів

Побудова реєстру активів за MAC, IP, банерами протоколів, версіями прошивок і ролями.

3.3.2. Інструменти і методики аналізу OT-трафіку

Wireshark

Дисектори для Modbus/TCP, S7, DNP3, IEC 104, EtherNet/IP, IEC 61850 MMS і GOOSE.

Фільтри на небезпечні функції наприклад, Modbus write multiple registers, S7 job functions.

Zeek і nDPI

Розширювані фреймворки для протокольних логів, видимість «хто з ким і про що» у довгій динаміці.

IDS для OT

Сигнатури і поведінкові моделі для виявлення відхилень у частоті опитування, нових майстрів на шині, аномальних функціональних кодів.

Обачність із активними інструментами

- Nmap і NSE-скрипти застосовувати лише у лабораторіях або під контролем змін.
- Modbus Poll, S7-клієнти та інші емулятори клієнтів використовувати для тестів у «пісочниці».

3.3.3. Операційні правила роботи з PCAP і телеметрією

Політика зберігання

Політика зберігання і доступу до PCAP, щоб не витікали технологічні секрети.

Санітарія даних

Санітарія даних персональні і комерційно чутливі поля маскуються перед передачею стороннім.

Маркування чутливості

Маркування чутливості і терміни зберігання з урахуванням нормативних вимог.

Розбори польотів

Регулярні розбори польотів з відтворенням інцидентів на основі захоплених сесій.

3.4. Підсумки та практичні рекомендації

Ключові висновки

- Більшість історичних OT-протоколів створені без урахування сучасних кіберзагроз.
- Перехід до IP, COTS і віртуалізації розширив поверхню атаки, але дав інструменти для захисту.
- Безпека досягається поєднанням архітектурних рішень, експлуатаційної дисципліни і безперервного моніторингу.

Рекомендації дій

- Провести інвентаризацію протоколів у зонній моделі, визначити «гарячі точки».
- Впровадити DPI-брандмауери на трактах OT і сегментацію з жорсткими ACL списками контролю доступу.
- Міграцію на протоколи з вбудованою безпекою планувати поетапно OPC UA, захищені профілі DNP3 SA, TLS-канали.
- Розгорнути пасивний моніторинг і інтегрувати OT-телеметрію до SOC.
- Регулярно перевіряти процедури резервування, відновлення і реагування на інциденти з урахуванням специфіки OT.

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!