Модуль 2. Пристрої та протоколи взаємодії систем ICS/SCADA

Лекція 1: Основні типи систем промислового контролю

Що розглянемо?

- Картина екосистеми промислової автоматизації та її ключові ролі
- Як влаштовані та взаємодіють SCADA, DCS, PLC, SIS
- Де з'являються кіберризики і які архітектурні принципи допомагають їх зменшити

Пояснення скорочень при першій появі

- ICS — Industrial Control Systems, промислові системи керування
- OT — Operational Technology, операційні технології
- IT — Information Technology, інформаційні технології

1.1. SCADA. Місце і завдання в промисловій екосистемі

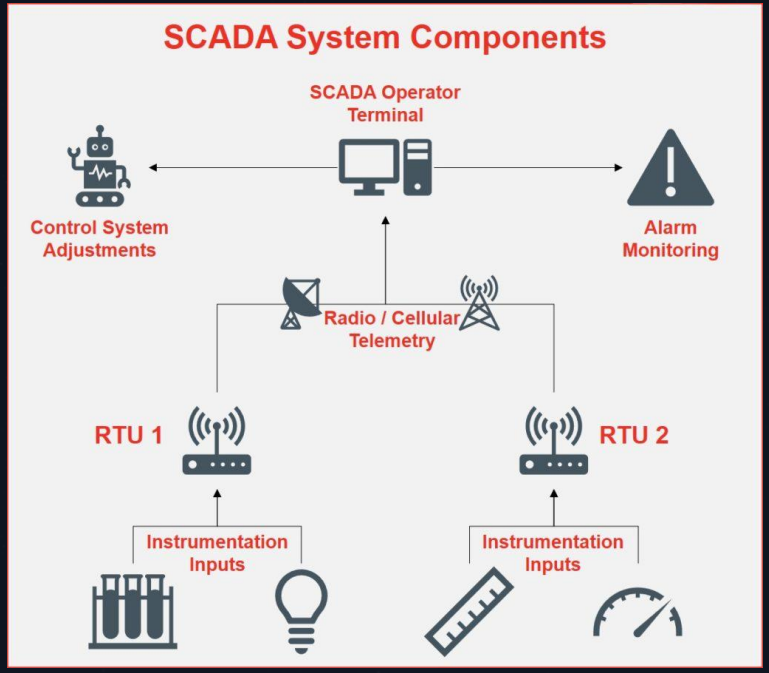
1.1.1. Що таке SCADA?

SCADA — Supervisory Control and Data Acquisition, диспетчерське керування і збір даних. Призначення полягає у моніторингу та дистанційному керуванні процесами, що рознесені географічно.

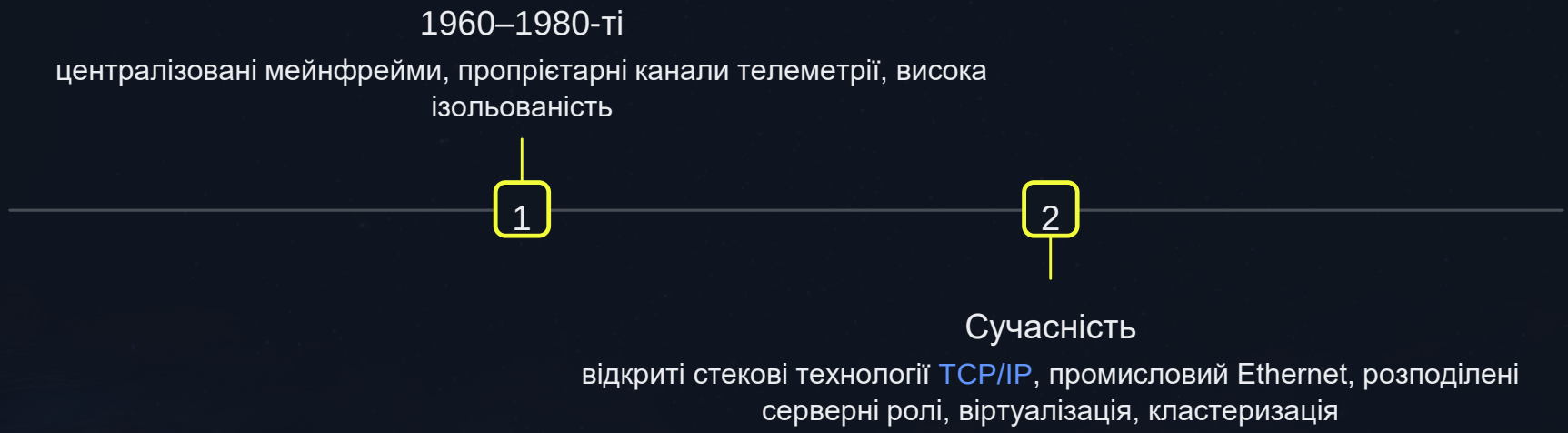
Приклади застосування: розподіл електроенергії, нафтогазотранспорт, водопостачання, транспортні мережі.

Відмінність від DAS — Data Acquisition System, суто збір даних без можливості відправляти команди керування.

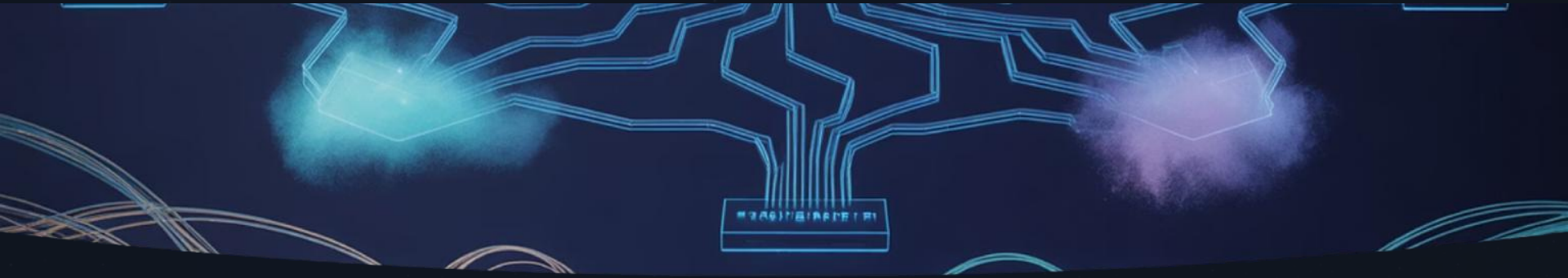
Ключова цінність для критичної інфраструктури полягає у підтриманні доступності послуг, скороченні часу реагування на відмови, централізованій видимості подій.



1.1.2. Еволюція SCADA. Від ізоляції до інтеграції



Зближення з IT полегшує інтеграцію з бізнес-аналітикою, але переносить і загальні IT-ризики у світ OT.



1.1.3. Архітектура SCADA високого рівня

Control Center
центр керування з локальною мережею LAN

Вузли на проммайданчиках
лінійні об'єкти з'єднані глобальною мережею WAN

Транспорт телеметрії: оптоволокно, мікрохвилі, радіорелейні лінії, стільникові та супутникові канали.

Потоки: опитування телеметрії, подієві сповіщення, аварійні тривоги, керувальні команди з підтвердженням.

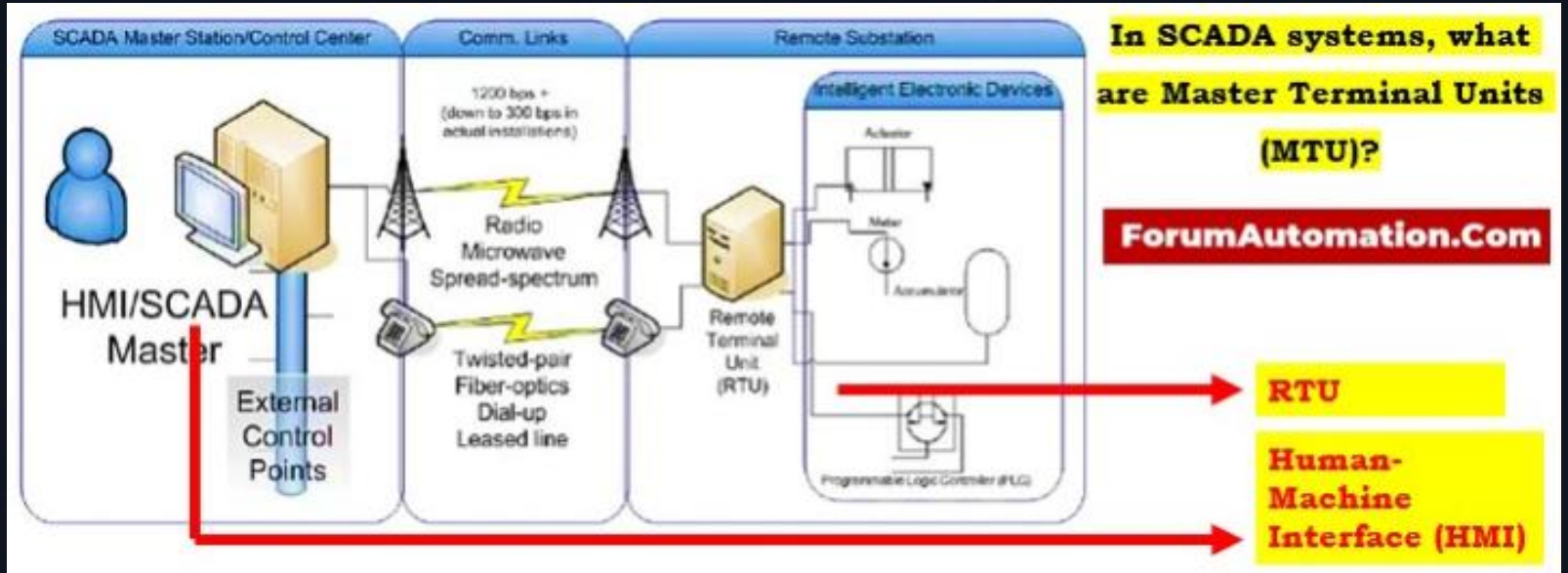
1.1.4. Компонент MTU. Серце SCADA

MTU — Master Terminal Unit, головний термінальний блок або SCADA-сервер.

Функції: збір, нормалізація і архівація даних, управління тривогами, маршрутизація команд, формування трендів і звітів.

Масштабування: підсистеми sub-MTU для розвантаження центрального ядра, гаряче резервування, реплікації баз даних.

Надійність: відмовостійкі кластери, резервні канали зв'язку, контроль цілісності конфігурацій.



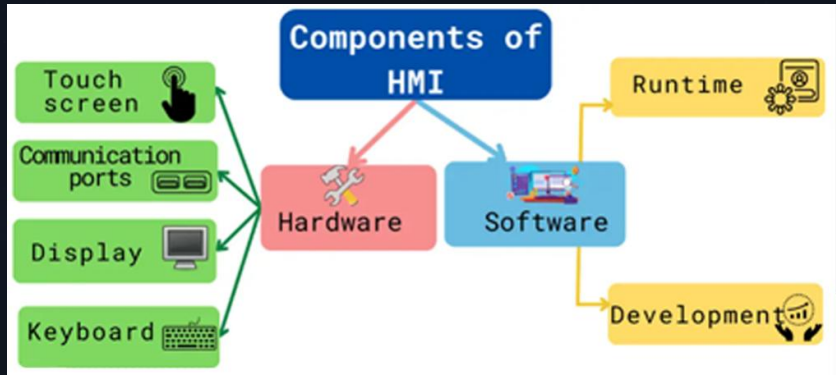
1.1.5. HMI. Людино-машинний інтерфейс і вимоги до проєктування

HMI — Human Machine Interface, операторські та інженерні консолі візуалізації.

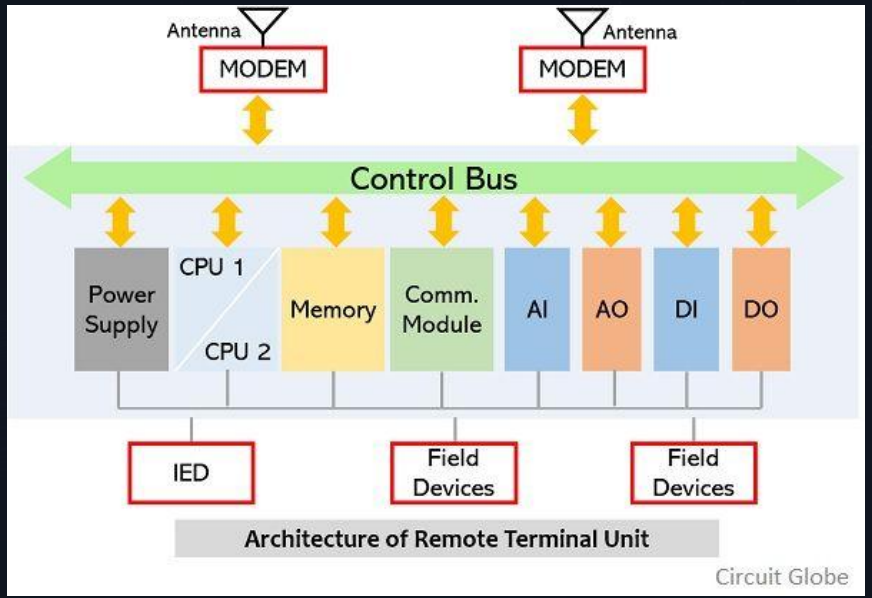
Призначення
відображення технологічних схем, підтвердження команд, робота з тривогами, аналіз трендів

Ергономіка
стандартизовані кольори і символи, пріоритизація тривог, сценарії підтвердження дій, журналювання

Захист
розділення ролей операторів та інженерів, багатофакторна автентифікація, контроль знімних носіїв, запис усіх дій



1.1.6. RTU. Польові «очі та руки»



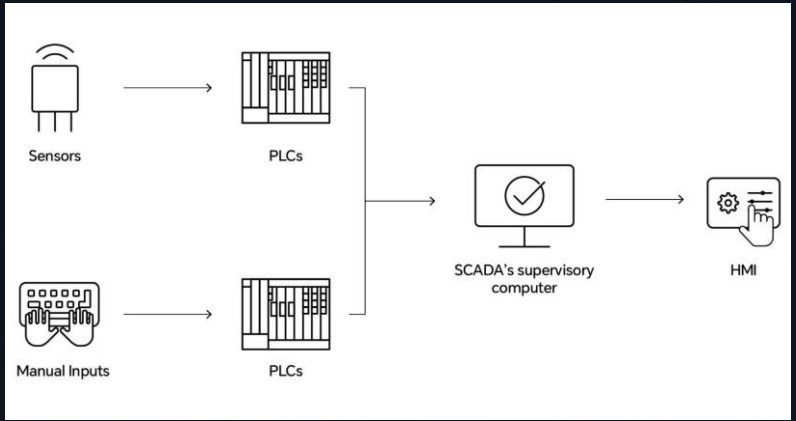
RTU — Remote Terminal Unit, віддалена термінальна одиниця в суворих умовах експлуатації.

Призначення: збір локальних показників, виконання простих логік, комутація приводів за командами центра.

Інтерфейси: багатопортові послідовні з'єднання, комунікації з периферією, живлення з резервом, захист від електромагнітних завад.

Переваги: подієве формування телеметрії зменшує трафік, локальні міжзахисти скорочують залежність від каналу.

1.1.7. PLC у контурі SCADA та взаємодія з IED



PLC — Programmable Logic Controller, програмований логічний контролер. Забезпечує близько-процесну швидкодію і детермінізм, у тому числі PID-регулювання, тобто пропорційно-інтегрально-диференціальне керування.

Режими RUN і PROGRAM з фізичним ключем-перемикачем для контролю змін.

IED — Intelligent Electronic Device, інтелектуальний електронний пристрій для захисту, вимірювань і автоматики в енергетиці, що взаємодіє з RTU/PLC.

1.1.8. Дані та історики. Фундамент аналітики

01

Data Historian

спеціалізована база для зберігання часових рядів з високою частотою опитування

02

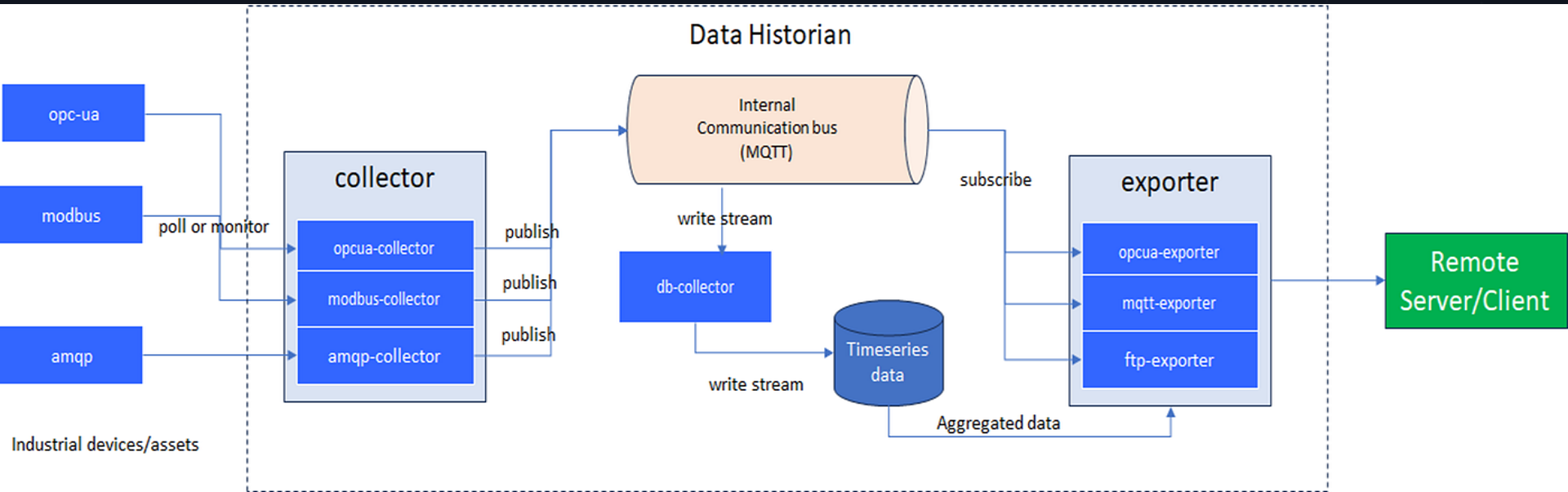
Можливості

стиск без втрат значущості, агрегації, SLA щодо доступності, інтерфейси до звітності і систем підтримки рішень

03

Якість даних

калібрування датчиків, виявлення пропусків, маркування некоректних значень, часові мітки джерела

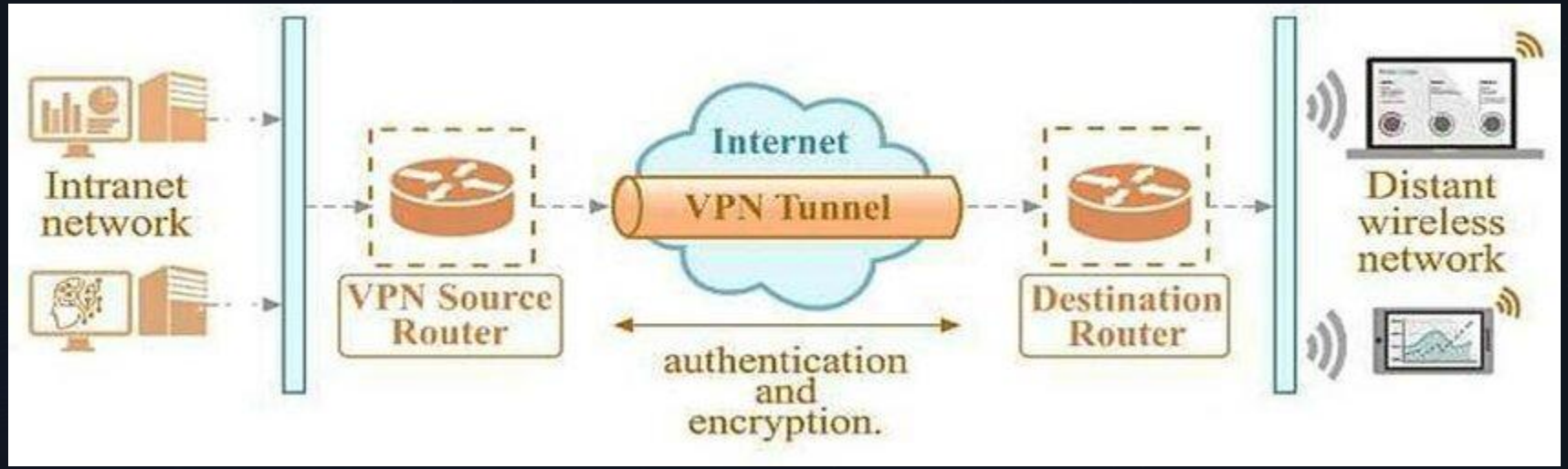


1.1.9. Мережеві канали SCADA і вимоги до якості

Канали WAN добирають з урахуванням затримок, втрат пакетів, стійкості до збоїв.

Пріоритет на оптоволокно і MPLS, радіо і супутник як резерв.

Для старих протоколів без захисту застосовують шифрування каналу і тунелювання з автентифікацією.



1.1.10. Кіберризики SCADA і архітектурні контрзаходи

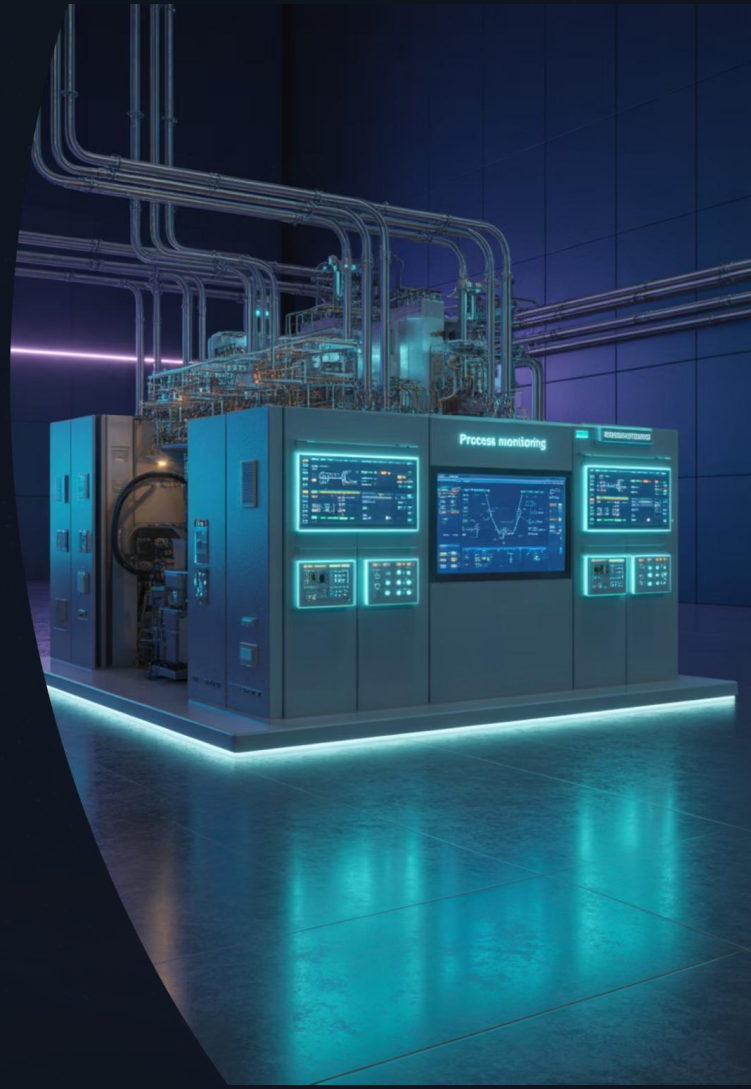
Типові загрози

застарілі протоколи без автентифікації, фішингові атаки на інженерні станції, транзиторні активи, несанкціоновані модеми

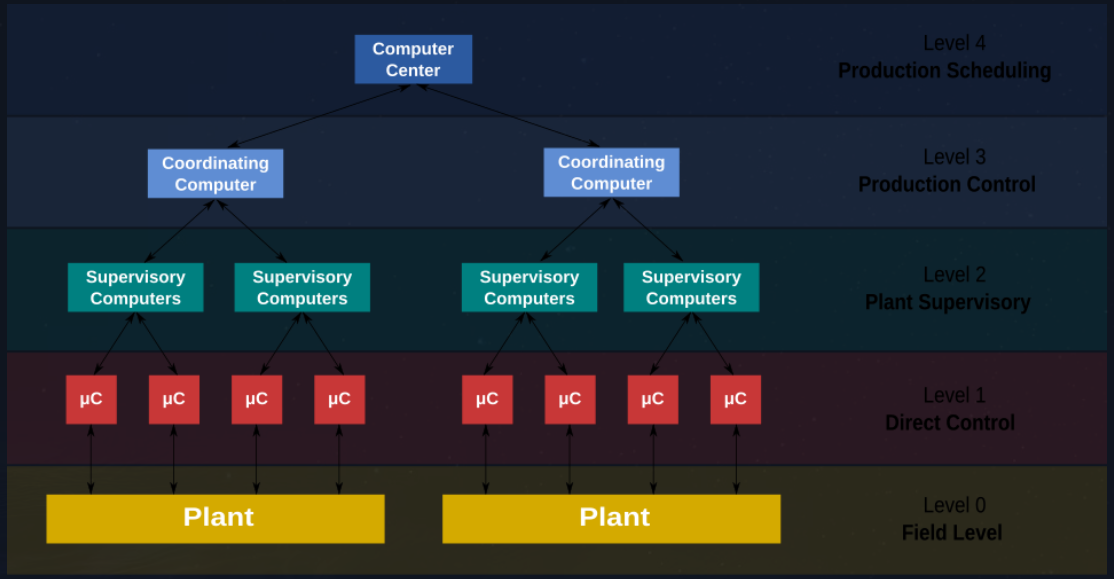
Контрзаходи

сегментація на зони та кондуїти, демілітаризована зона DMZ між OT і IT, моніторинг мережі за допомогою NIDS — Network Intrusion Detection System, суворий контроль змін, політика резервних копій і відновлення, регламенти для знімних носіїв

1.2. DCS. Системи розподіленого керування



1.2.1. Що таке DCS?



DCS — Distributed Control System, розподілена система керування для автоматизації комплексних процесів у межах одного майданчика.

Фокус на керуванні замкненими контурами, детермінізмі та низькій затримці.

На відміну від SCADA працює переважно з локальною мережею LAN з високою пропускною здатністю і надійністю.

1.2.2. Архітектура DCS і промислові шини

Розподілені контролери

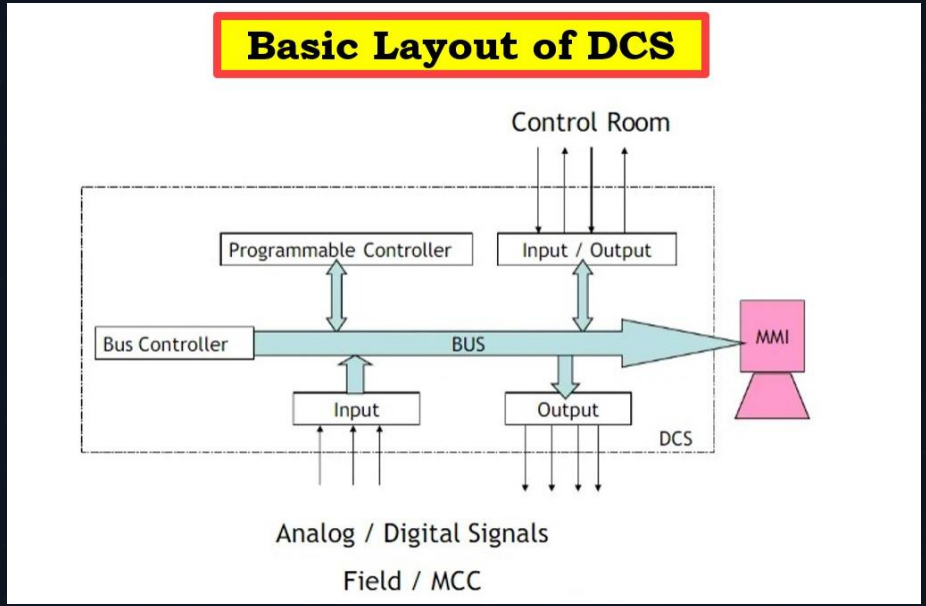
з резервуванням центральних процесорів та двохканальними мережами

Польові шини

промислові Ethernet-технології, зокрема PROFIBUS/PROFINET, Foundation Fieldbus, HART

Сервери

тривог і історіків, інженерні станції з централізованим управлінням версіями, єдина модель даних

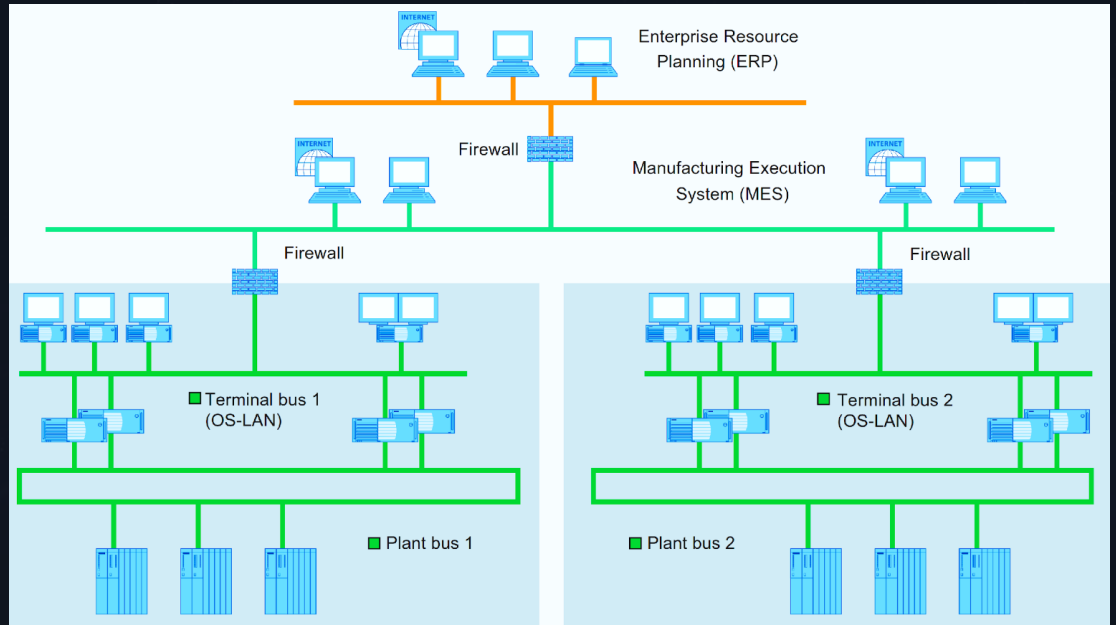


1.2.3. Кібербезпека DCS. Практичні підходи

Архітектура із розподілом на виробничі зони, застосування зворотних проксі та односторонніх шлюзів у DMZ.

Списки контролю доступу ACL за принципом заборонити все і дозволяти точково, мінімізація сервісів на контролерах.

Пасивна видимість мережі, тестові середовища для патчів, білі списки застосунків на інженерних станціях, контроль USB і Bluetooth.



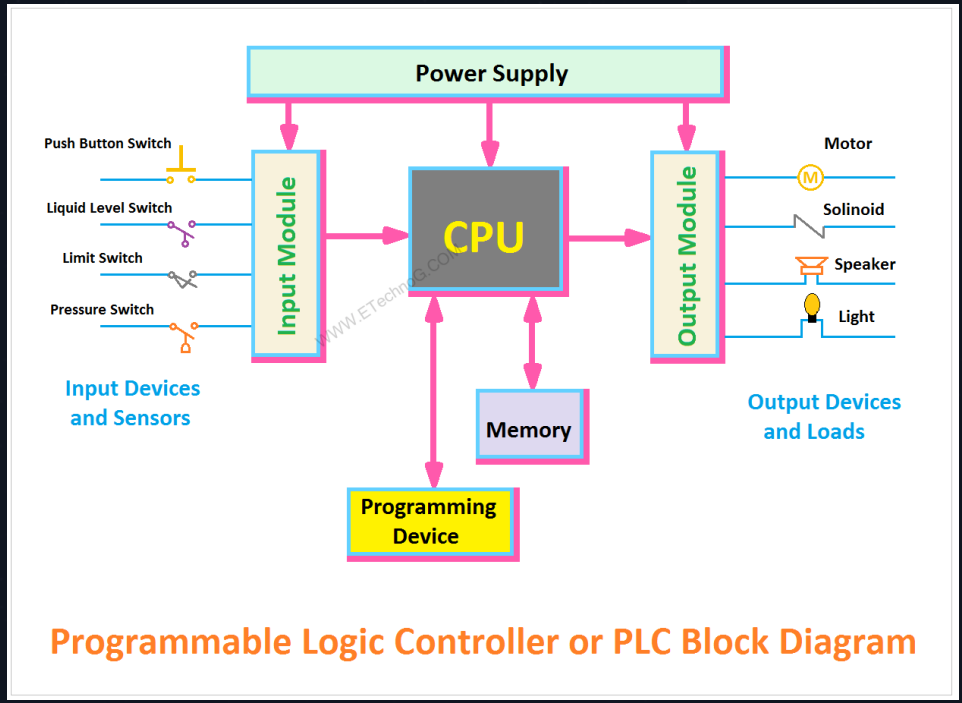
1.3. PLC. Базовий контролер реального часу

1.3.1. Що таке PLC

PLC реалізує цикл опитування входів, виконання логіки і встановлення виходів з гарантованою періодикою.

Функції: дискретні і аналогові входи-виходи, логічні операції, таймери і лічільники, PID, обміни з HMI та верхніми рівнями.

Вимоги: робота у важких умовах, прогнозований час циклу, довгий життєвий цикл обладнання.



1.3.2. Програмування PLC за IEC 61131-3

Мови програмування

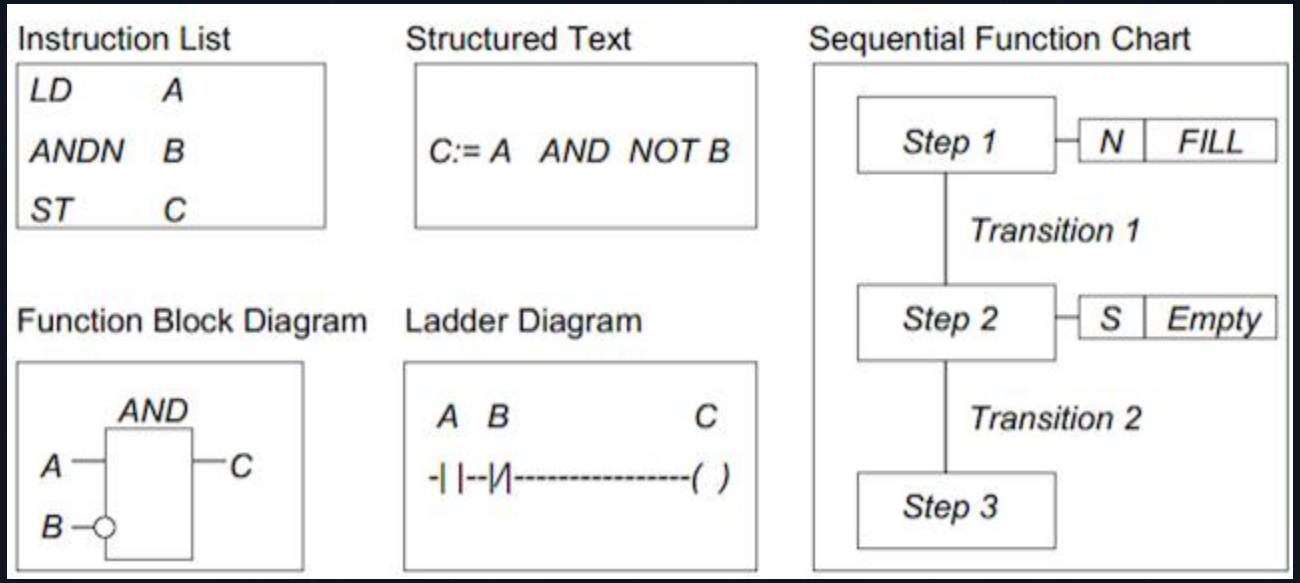
Relay Ladder Logic, Function Block Diagram, Structured Text, Sequential Function Chart, Instruction List

Переваги стандарту

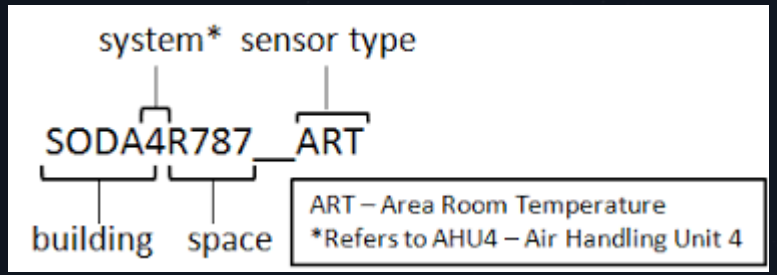
Портативність логіки і міжвендорна сумісність інструментів конфігурації

Практики

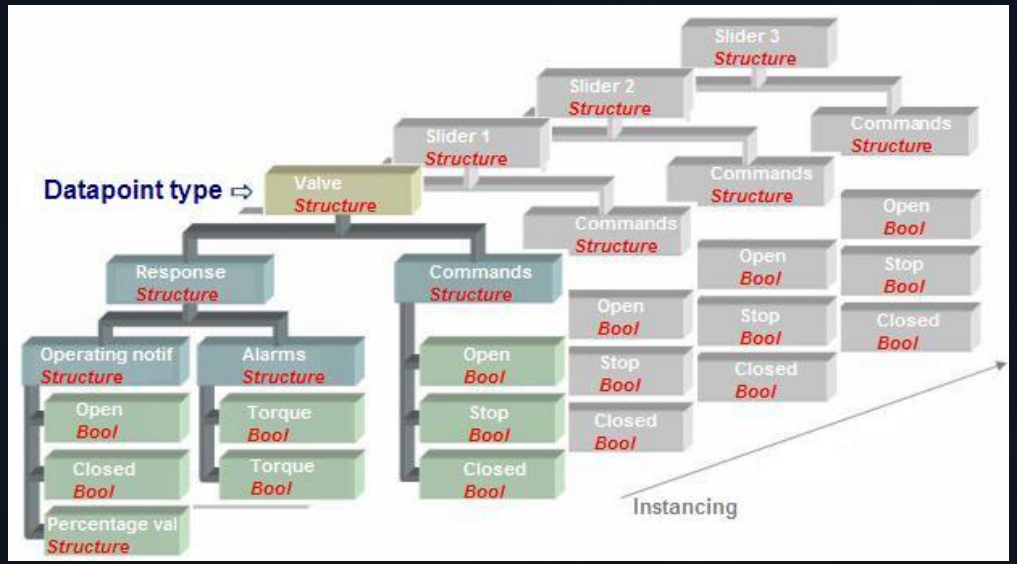
контроль версій, підпис пакунків, обов'язкові стендові випробування перед введенням у експлуатацію



1.3.3. Точки і теги. Єдина мова даних



«Точки» відповідають фізичним сигналам або віртуальним змінним, «теги» надають людям читабельні імена.



Принципи неймінгу: коди цехів і установок, класи обладнання, тип сигналу, одиниці виміру.

Узгодженість тегів спрощує інженерні роботи, аналіз історії і міжсистемну інтеграцію.

1.3.4. Режими безпеки і фізичні запобіжники на PLC

01

Фізичний контроль

Режими RUN та PROGRAM з механічним ключем-перемикачем, що унеможливлює несанкціоноване оновлення прошивок і логіки

02

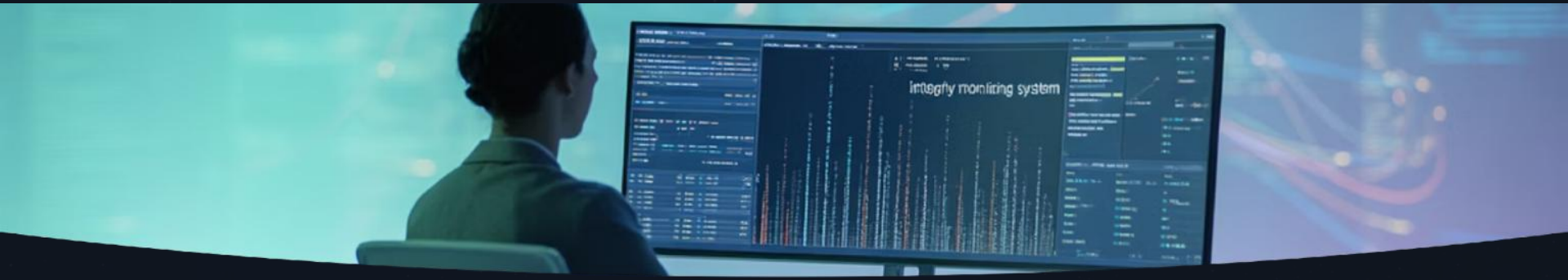
Контроль доступу

Розділення облікових записів для інженерів і операторів, багатофакторна автентифікація, повне журналювання змін, контроль сесій віддаленого доступу

03

Перевірка цілісності

Регулярні огляди логіки з підтвердженням цифрових підписів і контрольної суми



1.3.5. Кіберзагрози до PLC і шляхи їх пом'якшення

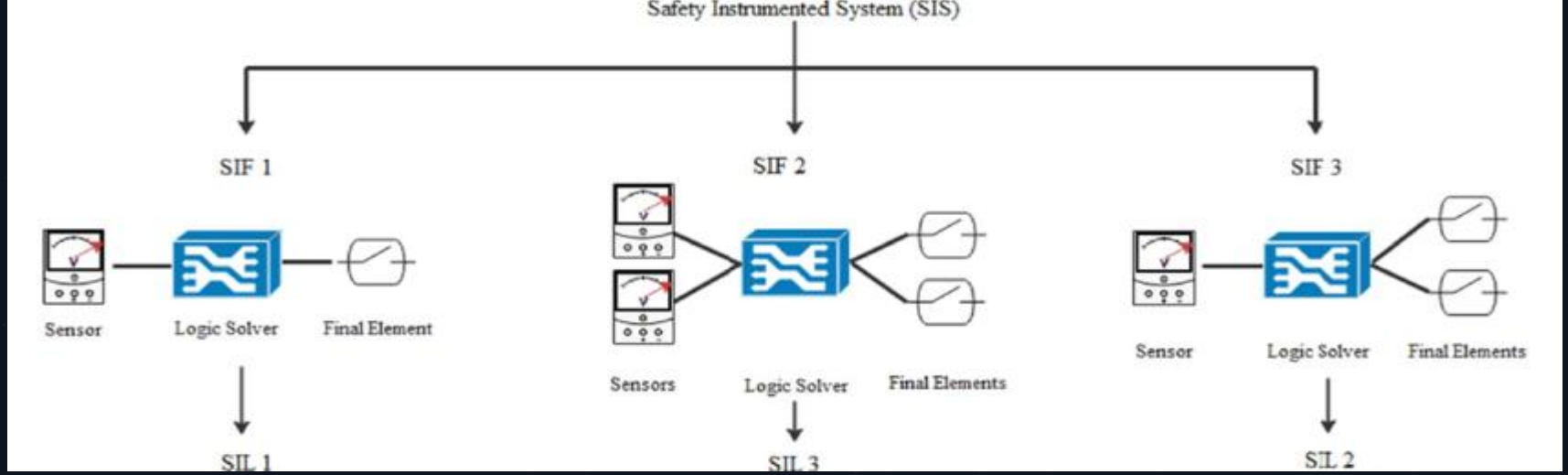
Загрози

Несанкціонована модифікація логіки, сторонні прошивки, небезпечні або застарілі служби, експлуатація незахищених протоколів.

Захист

міжмережеві екрани на рівні осередків, білі списки мережевих маршрутів, підписані оновлення, періодична перевірка цілісності, окремі середовища для тестів

1.4. SIS. Системи інструментальної безпеки



1.4.1. Що таке SIS?

SIS — Safety Instrumented System, відмовна система, що переводить процес у безпечний стан за настання небезпечної події.

Працює поруч з BPCS — Basic Process Control System, але фізично і логічно ізольовано для виключення спільних точок відмов.

SIL — Safety Integrity Level, показник цілісності функцій безпеки. SL — Security Level, рівень кіберзахисту. Ці поняття незалежні і оцінюються окремо.

1.4.2. Кібербезпека SIS. Уроки інцидентів і вимоги до ізоляції

Інциденти класу HatMan TRITON TRISIS продемонстрували ризик цілеспрямованих атак на контролери безпеки.

Фізичне відокремлення

мереж SIS, односторонні шлюзи для передачі телеметрії

Незалежні станції

інженерні станції, окремі облікові записи, обмеження сервісів до мінімально необхідних

Регулярні перевірки

функцій SIF — Safety Instrumented Function, з фіксацією результатів і аналізом відхилень

1.4.3. Інтеграція функціональної безпеки і кібербезпеки

Єдиний реєстр змін, спільні аудити, узгоджені критерії приймання робіт.

Координація команд безпеки процесу і кіберзахисту протягом усього життєвого циклу.

Взаємні вимоги: кіберконтрзаходи не повинні погіршувати функціональну безпеку, а заходи safety не мають блокувати механізми кіберзахисту.

1.5. Підсумки

Системи керування

SCADA дає централізоване керування розподіленими активами, DCS керує щільними процесами майданчика, PLC забезпечує швидкодіючий локальний контроль, SIS гарантує безпечний стан процесу

Архітектура і процеси

експлуатації мають визначати рівень кіберзахисту не менше, ніж самі технології

Базові принципи

Сегментація на зони і кондуїти, DMZ між OT і IT, контроль змін і видимість мереж є базовими для всіх розглянутих типів систем

Пріоритети OT

доступності і цілісності даних у OT середовищі визначає вибір рішень, налаштувань і методів експлуатації

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!