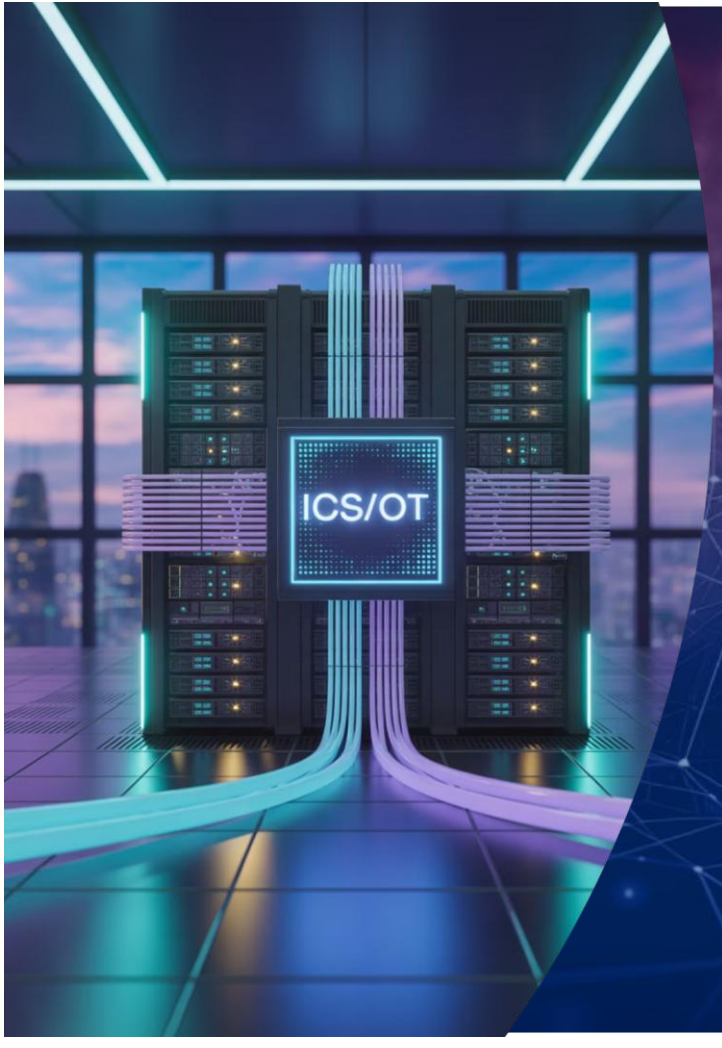


Модуль 1. Основи управління кібербезпекою

Лекція 2: Стандарти та фреймворки кібербезпеки для ICS/SCADA

Мета лекції

Практична картина ландшафту

Сформувати практичну картину ландшафту стандартів для ICS (Industrial Control Systems — промислові системи керування) і SCADA (Supervisory Control and Data Acquisition — диспетчерське керування і збір даних).

Роль ISA/IEC 62443

Пояснити місце та роль ISA/IEC 62443 як базового фреймворку для OT (Operational Technology — операційні технології).

Порівняння підходів

Порівняти підходи NIST SP 800-82, NERC CIP, ISO/IEC 27000 та показати, як поєднувати SL (Security Levels — рівні безпеки) і ML (Maturity Levels — рівні зрілості).

План і результати навчання

Що розглянемо

- Ландшафт стандартів ICS/OT і роль корпоративних фреймворків.
- Серію ISA/IEC 62443 та її чотири частини від термінів до вимог для компонентів.
- Дві фундаментальні концепції: «Захист в глибину» і «Зони та тракти».
- Огляд NIST SP 800-82, NERC CIP, ISO/IEC 27000 з акцентом на застосовність.
- Практика використання SL і ML у проектуванні та аудиті.

Що вмітимете

- Побудувати дорожню карту впровадження 62443.
- Обрати й поєднати стандарти під свою галузь і регуляторні вимоги.
- Визначити SL-T (цільовий рівень безпеки) для зон та оцінити організаційний ML.

2.1. Призначення та важливість ISA/IEC 62443

2.1.1. Ландшафт стандартів для ICS і OT

Контекст

- OT має інші пріоритети ніж IT, головним є доступність технологічного процесу та безпека людей.
- Норми поділяються на регуляторні обов'язкові та добровільні рекомендаційні.

Ключові джерела

- ISA/IEC 62443 як системний фреймворк для IACS (Industrial Automation and Control Systems — системи промислової автоматизації та керування).
- NIST SP 800-82 як практичний гід для безпечної архітектури і контролів.
- NERC CIP як обов'язкова база для енергетики Північної Америки.
- ISO/IEC 27000 як основа ISMS (Information Security Management System — система управління інформаційною безпекою) у бізнесі.

2.1.2. ISA/IEC 62443 як «золотий стандарт» для IACS

Призначення

Забезпечити гнучку структуру протидії чинним і майбутнім загрозам для IACS з урахуванням безпеки процесу, доступності, цілісності та конфіденційності.

Сфера застосування

Виробництво, нафтогаз і хімія, енергетика, вода, харчова промисловість, фарма.

Можлива адаптація до інших доменів, зокрема мобільності та медичних приладів.

Практичні переваги

Спільна мова для власника активів, інтегратора і постачальника.

Прозорий перехід від політик до технічних вимог і компонентів.

2.1.3. Походження і розвиток серії 62443

Походження

Розпочато як ISA-99 під егідою ISA, далі прийнято IEC.

Розробляється IEC TC65 WG10 із залученням промисловості та експертів OT.

Актуальність

Регулярні оновлення з урахуванням нових технік атак, зокрема на ланцюг постачання і віддалений доступ.

Підтримка технічними звітами та довідниками для практичного впровадження.

2.1.4. Ролі та відповідальність у 62443

Власник активів

Визначає політики, приймає ризики, затверджує CSMS (Cybersecurity Management System — система управління кібербезпекою) і цільові SL-T.

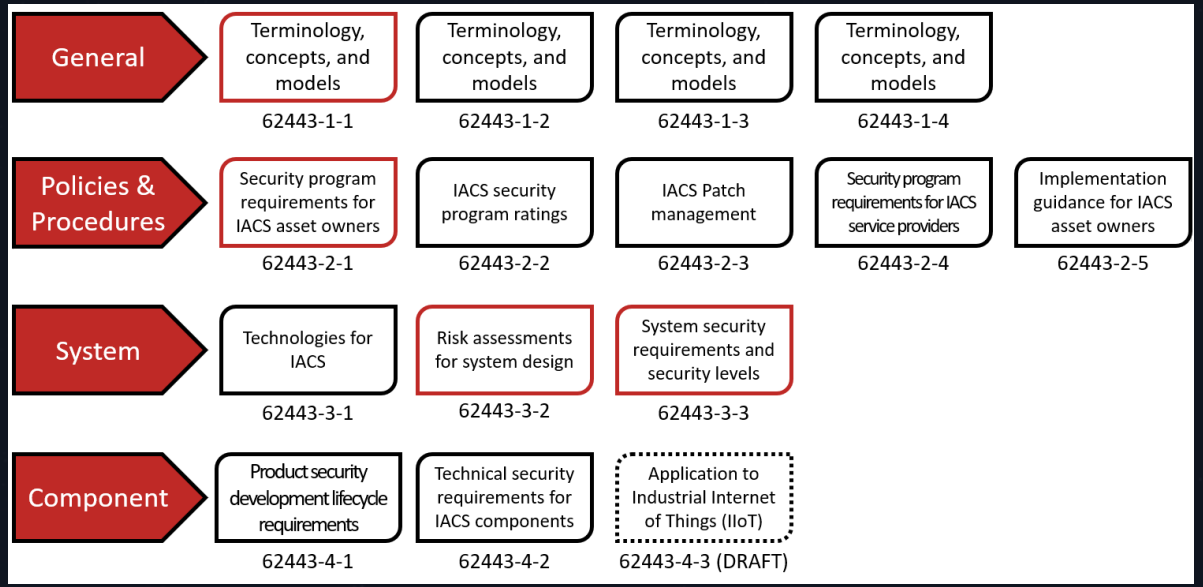
Системний інтегратор

Проектує архітектуру зон та трактів, впроваджує контролі, проводить валідацію SL-A (досягнутий рівень).

Постачальник продукту

Дотримується IEC 62443-4-1 щодо життєвого циклу безпечної розробки, забезпечує функції безпеки згідно IEC 62443-4-2.

2.2. Структура серії ISA/IEC 62443



2.2.1. Структура серії 62443: чотири частини

Загальний рівень (Part 1)

Термінологія, моделі, метрики відповідності, глосарій.

Рівень систем управління (Part 2)

Політики, процедури, програми безпеки, управління патчами, вимоги до провайдерів послуг.

Рівень систем (Part 3)

Вимоги до архітектури, ризик-орієнтоване проектування, рівні безпеки для систем.

Рівень компонентів (Part 4)

Вимоги до компонентів і життєвого циклу безпечної розробки.

2.2.2. Part 1. Терміни, моделі, метрики

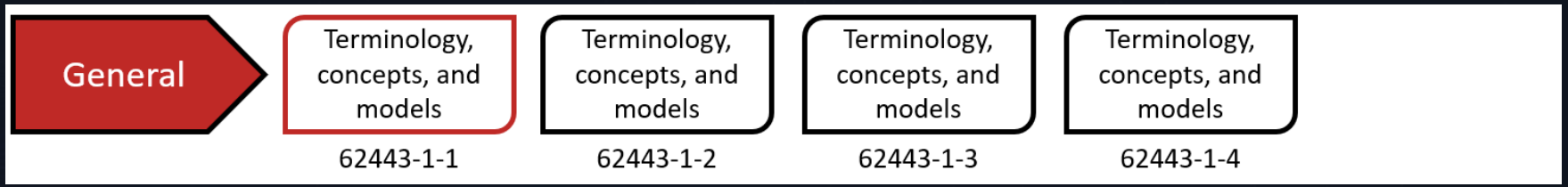
Що містить

- **IEC TS 62443-1-1** терміни, концепції і моделі.
- **IEC TR 62443-1-2** глосарій.
- **IEC 62443-1-3** метрики відповідності до FR (Foundational Requirements — базові вимоги) і SR (System Requirements — системні вимоги).
- **IEC TR 62443-1-4** життєвий цикл і типові сценарії.

Практична цінність

Єдина термінологія для всіх учасників.

Можливість кількісно вимірювати відповідність архітектури вимогам.



2.2.3. Part 2. Політики, процедури, CSMS

Що містить

- **IEC 62443-2-1** створення програми безпеки OT і узгодження з ISO/IEC 27001.
- **IEC TR 62443-2-2** орієнтири рівнів захисту.
- **IEC TR 62443-2-3** управління патчами у середовищах з високою доступністю.
- **IEC 62443-2-4** вимоги до постачальників послуг IACS.
- **IEC TR 62443-2-5** практичні настанови для власників активів.

2.2.4. Part 3. Вимоги та проектування систем

Що містить

- **IEC TR 62443-3-1** огляд технологій безпеки для OT.
- **IEC 62443-3-2** методика оцінювання ризиків і проектування зон з трактами.
- **IEC 62443-3-3** вимоги до систем і прив'язка до рівнів безпеки SL.

Практичний вихід

Карта зон і трактів, вимоги до ідентифікації, автентифікації, авторизації, журналювання, цілісності, доступності.

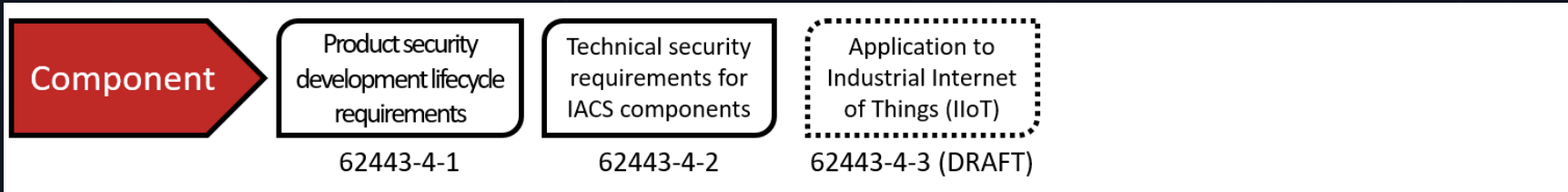
2.2.5. Part 4. Вимоги до компонентів і SDL

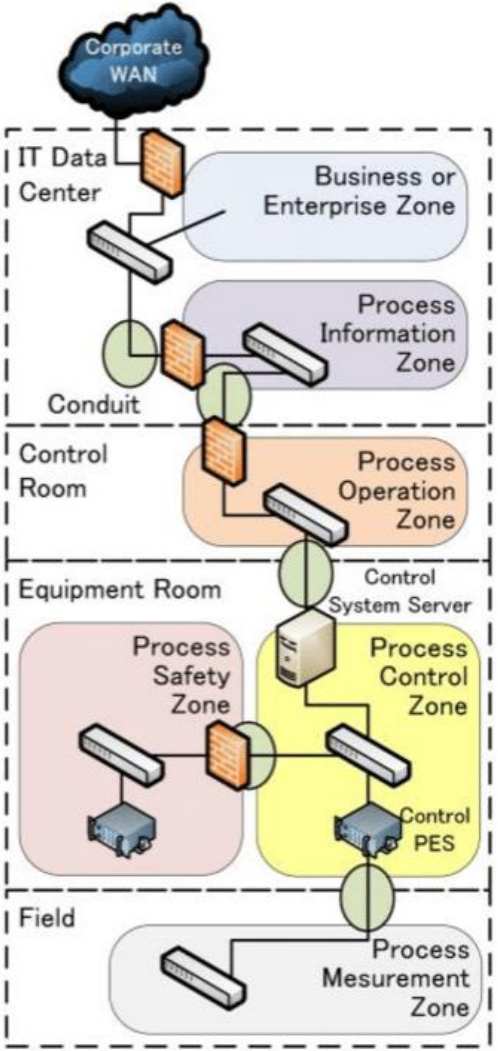
Що містить

- **IEC 62443-4-1** вимоги до SDL (Secure Development Lifecycle — життєвий цикл безпечної розробки).
- **IEC 62443-4-2** технічні вимоги до вбудованих, хостових, мережевих і прикладних компонентів.

Український контекст

IEC 62443-4-2 прийнято як ДСТУ, що спрощує закупівлі і сертифікацію.





2.3. Ключові концепції ISA/IEC 62443

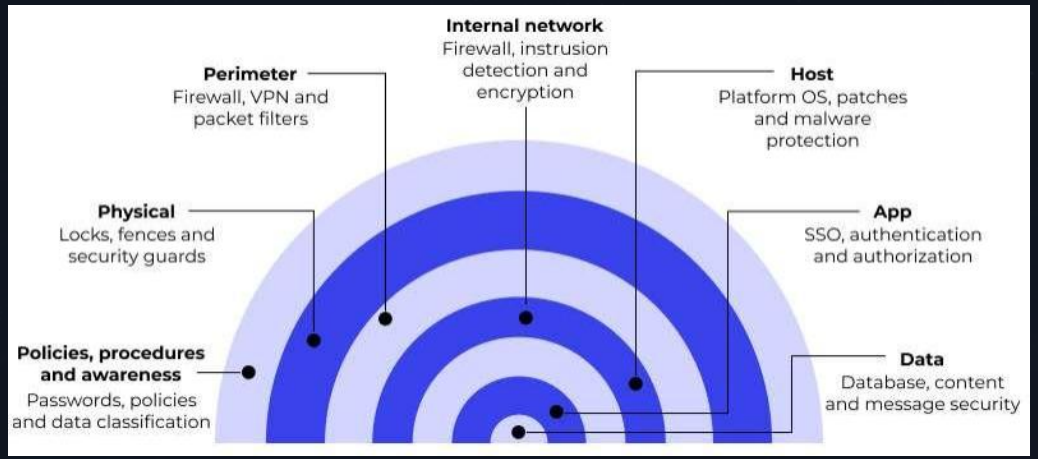
2.3.1. Захист в глибину

Суть

Багатошарова оборона, де компрометація одного рубежу не веде до критичного інциденту.

Реалізація

- Політики і процеси на керівному рівні.
- Сегментація мереж і міжмережеві екрани між зонами.
- Контроль застосунків і вайтлістинг на хостах.
- Шифрування каналів і взаємна автентифікація.
- Моніторинг у SIEM (Security Information and Event Management — керування подіями безпеки) і OT-орієнтовані IDS/NIDS.



2.3.2. Зони та тракти

Суть

Зона це група активів зі спільними вимогами безпеки і однорідним ризиком.

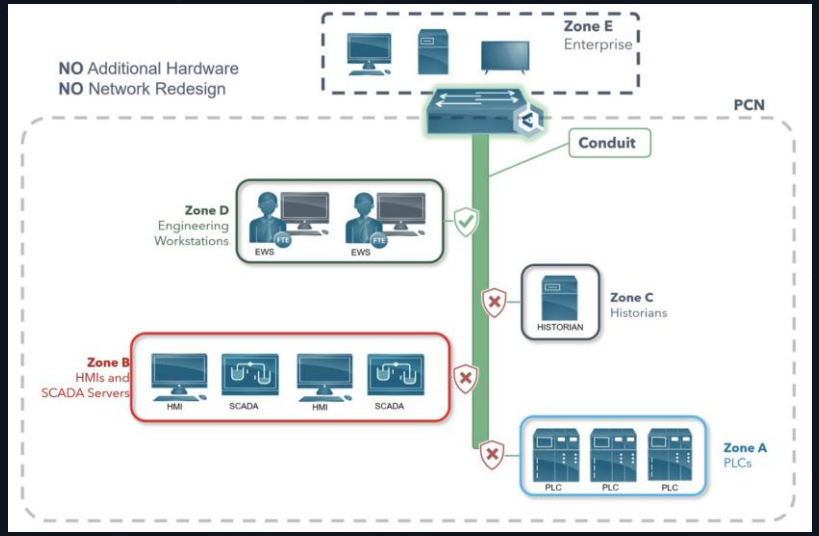
Тракт це керований шлях обміну між зонами з контролем доступу, цілісності і конфіденційності трафіку.

Практичні кроки

Класифікувати активи за критичністю процесу і впливом на безпеку.

Провести мінімізацію зв'язності і дозволити лише необхідні потоки.

Розмістити інспектори OT-протоколів на межах трактів.



2.3.3. Дорожня карта впровадження 62443

Інвентаризація IACS
Інвентаризація IACS, побудова карти активів.

Визначення зон і трактів
Визначення зон і трактів, моделювання загроз, оцінювання ризиків.

Встановлення SL-T
Встановлення SL-T для кожної зони.

Вибір контролів
Вибір контролів і компонентів, що відповідають IEC 62443-4-2.

Побудова CSMS
Побудова CSMS, узгодженого з ISO/IEC 27001.

Тести відповідності
Тести відповідності, аудит постачальників за IEC 62443-2-4 і IEC 62443-4-1.

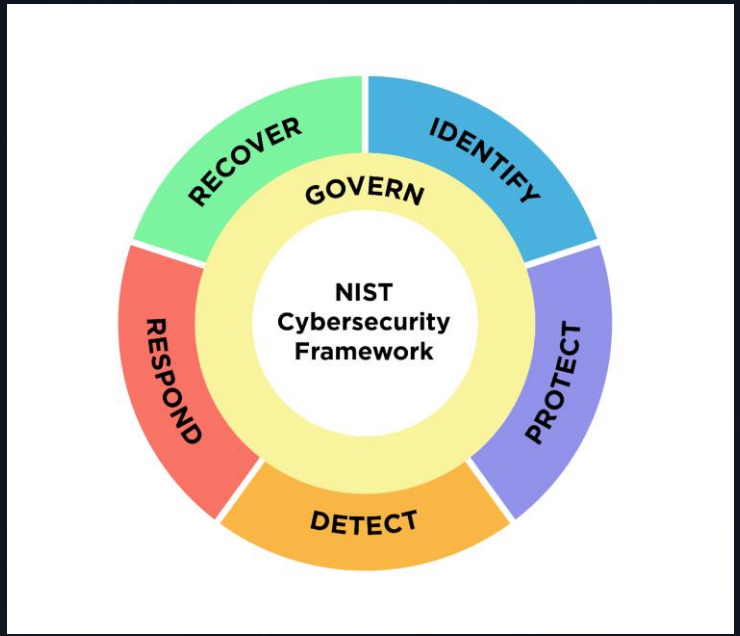
2.3.4. NIST SP 800-82. Посібник для ICS

Що дає

- Огляд топологій SCADA, DCS, PLC.
- Типові загрози і вразливості, базові архітектури і контролі.
- Взаємодія з NIST SP 800-53 як накладання контролів для федеральних систем.

Чому зручно

Простий для старту програм OT-безпеки, зрозумілі рекомендації і приклади архітектур.



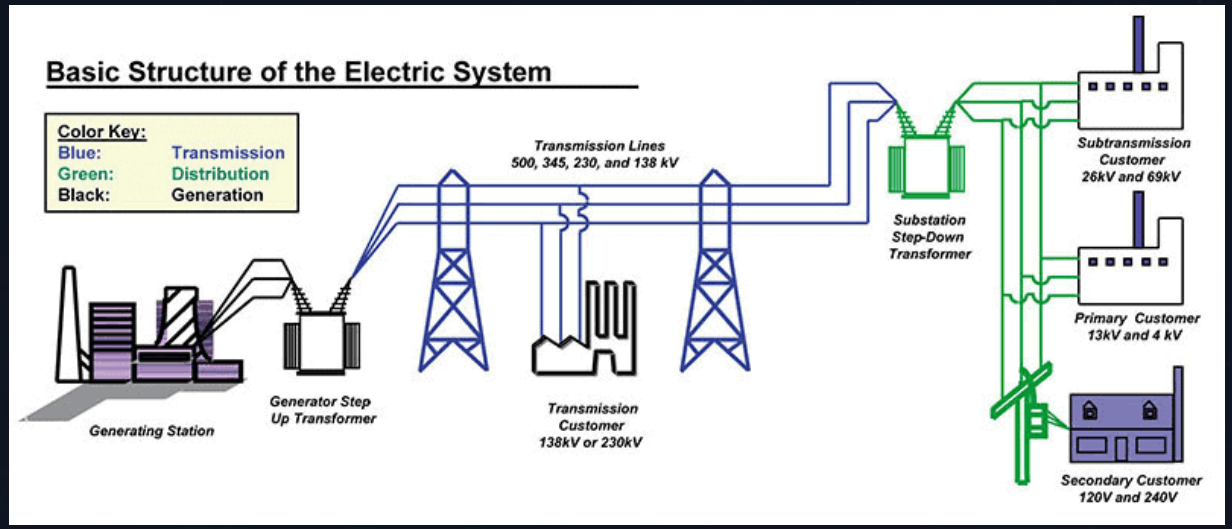
2.3.5. NERC CIP. Регуляція енергосектору

Призначення

Стандарти для BES (Bulk Electric System — об'єднана електроенергетична система) щодо кіберзахисту генерації і передачі.

Ключові вимоги

Електронні периметри, категоризація критичних кібератів, управління доступом, інцидент-респонс, навчання персоналу, аудит.



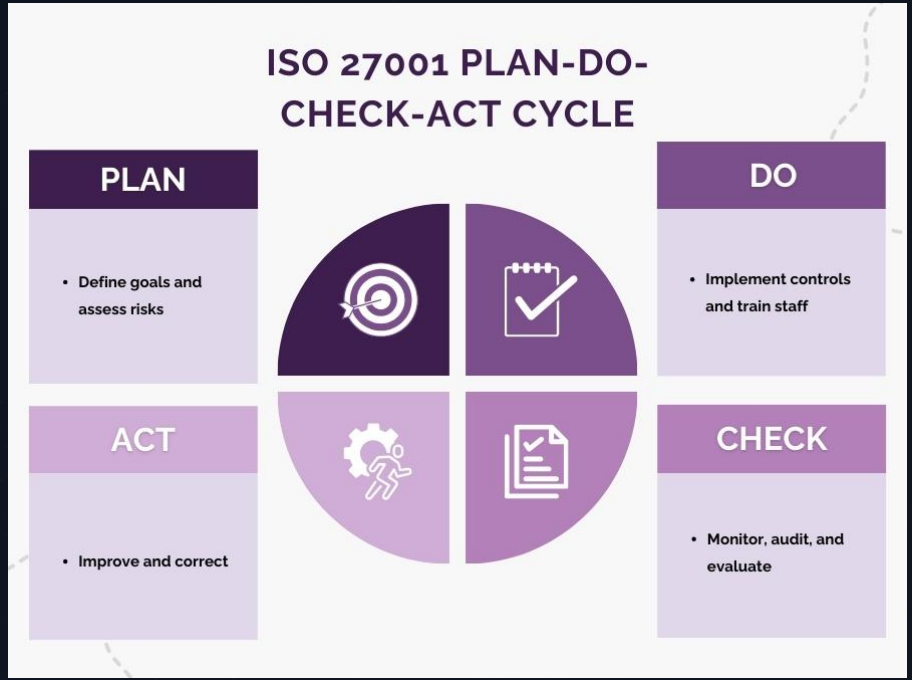
2.3.6. ISO/IEC 27000. Роль ISMS у підтримці OT

Що покриває

- ISO/IEC 27001 вимоги до побудови і вдосконалення ISMS.
- ISO/IEC 27002 каталог практичних контролів.

Як поєднати з OT

- Узгодити з IEC 62443-2-1 для політик і процесів.
- Адаптувати контролі до вимог реального часу, сегментації, відмовостійкості.



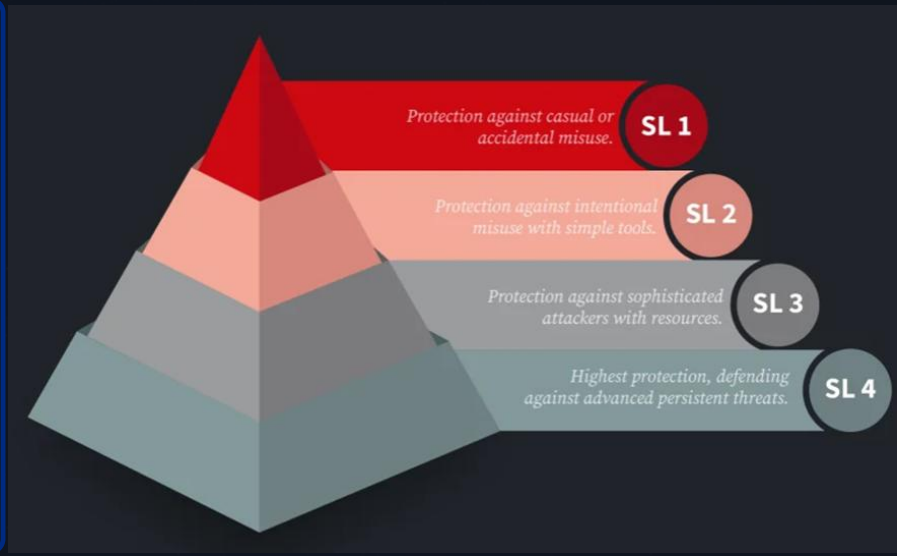
2.3.7. Рівні безпеки SL

Призначення

Орієнтир для добору контролів за зоною ризику.

Рівні

- SL 1 протидія випадковим діям і простим помилкам.
- SL 2 протидія супернику з базовими навичками і низькими ресурсами.
- SL 3 протидія фаховому супернику з помірними ресурсами і OT-компетенціями.
- SL 4 протидія високоресурсному і мотивованому противнику.



2.3.8. Застосування SL у проектуванні і закупівлях

Практика

01

Встановити SL-T

Встановити SL-T для кожної зони на базі оцінки ризиків.

02

Обирати компоненти

Обирати компоненти, що підтверджують можливості безпеки за IEC 62443-4-2.

03

Перевіряти SL-A

Перевіряти SL-A тестами, аудитами і безперервним моніторингом.

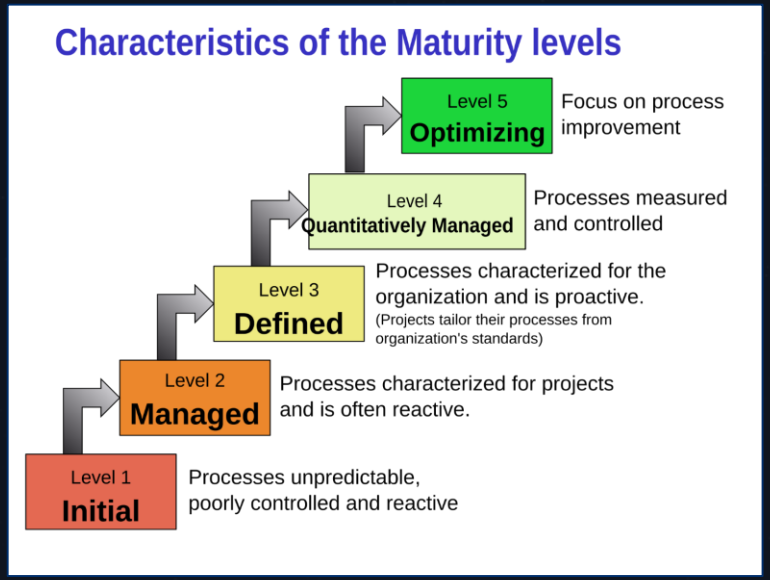
2.3.9. Рівні зрілості ML

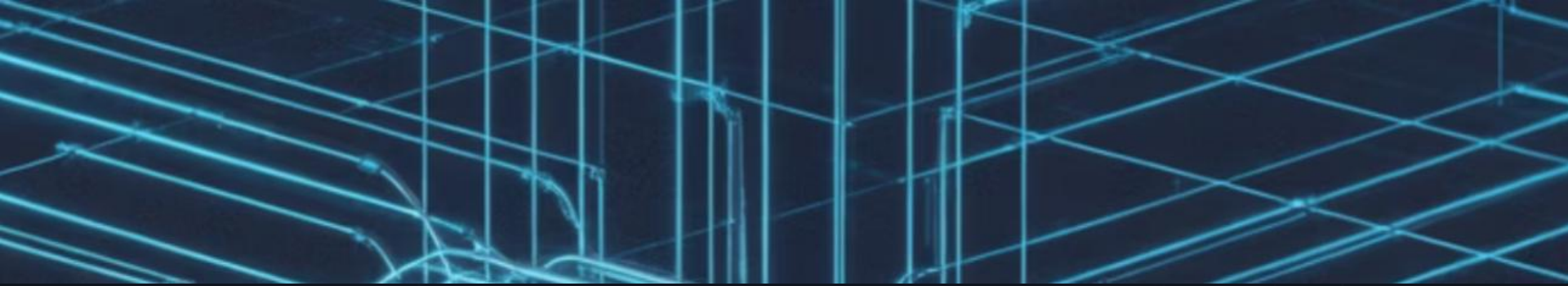
Суть

ML базується на CMMI-SVC (Capability Maturity Model Integration for Services — модель зрілості інтеграції сервісів) і оцінює процесну спроможність.

Рівні

- ML 1 виконання без стабільного процесу.
- ML 2 керовані процеси з доказами досвіду.
- ML 3 стандартизовані процеси і навчений персонал.
- ML 4 безперервне вдосконалення, внутрішні аудити, метрики.





2.3.10. Як поєднати SL і ML у реальному проєкті

Логіка

SL відповідає на питання що і як захищати технічно.

ML показує чи здатна організація стабільно підтримувати ці контролі.

Кроки

Задати SL-T по зонах, провести gap-аналіз до SL-A.

Оцінити ML для CSMS і постачальників, скласти план підвищення.

Пов'язати закупівлі і контракти з вимогами до SL компонентів і ML процесів.

2.4. Висновки та рекомендації

Висновки

- ISA/IEC 62443 дає повний цикл від політик до компонентів і узгоджується з корпоративним ISMS.
- NIST SP 800-82 спрощує старт і надає приклади архітектур.
- NERC CIP обов'язковий у BES, ISO/IEC 27000 структурує управління.

Дії

- Побудуйте карту зон і трактів, встановіть SL-T, оформіть CSMS.
- Вимагайте у постачальників відповідність IEC 62443-4-1 і технічні можливості IEC 62443-4-2.
- Використовуйте аудити і моніторинг для підтвердження SL-A і підвищення ML.
- Переглядайте політики і вимоги відповідно до змін загроз і технологій.

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.