Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
"XLI науково-технічна конференція молодих вчених та спеціалістів"

С.Я. Гільгурт, О.Г. Кіслов, В.М. Попова

Апаратне прискорення виявлення атак на цифрові підстанції

17.05.23 р.

Цифровізація промислових систем автоматизації

Переваги застосування IT-технологій:

- стандартизація;
- відпрацьованість технічних рішень;
- невисока вартість володіння;
- простота обслуговування.

Головний недолік: успадкована від IT **кібернебезпека**

Популярний раніше принцип "**Безпека через неясність**" ("Security through obscurity"), що полягає в досягненні інформаційної безпеки шляхом приховування внутрішнього устрою системи і особливостей її реалізації, вже не відповідає реаліям часу.

Наскільки досвід кіберзахисту в галузі IT придатний для промислових систем?

Одна з відмінністей: обмежені обчислювальні ресурси цифрових пристроїв, що використовуються в Smart Grid та SCADA-системах.

Тому важко оновлювати ПЗ та firmware, використовувати традиційні міжмережеві екрани, антивіруси та стеми виявлення вторгнень (СВВ).

Складнощі цифровізації електричних підстанцій – – передумови створення стандарту МЕК-61850

Життєвий цикл **силового обладнання** (трансформатори, комутаційні апарати, роз'єднувачі …) - близько **40 років**;

Життєвий цикл **керуючих систем** - близько **15 років**.

Типова ситуація, коли в єдиному комплексі змушені взаємодіяти пристрої декількох поколінь, не сумісні між собою.

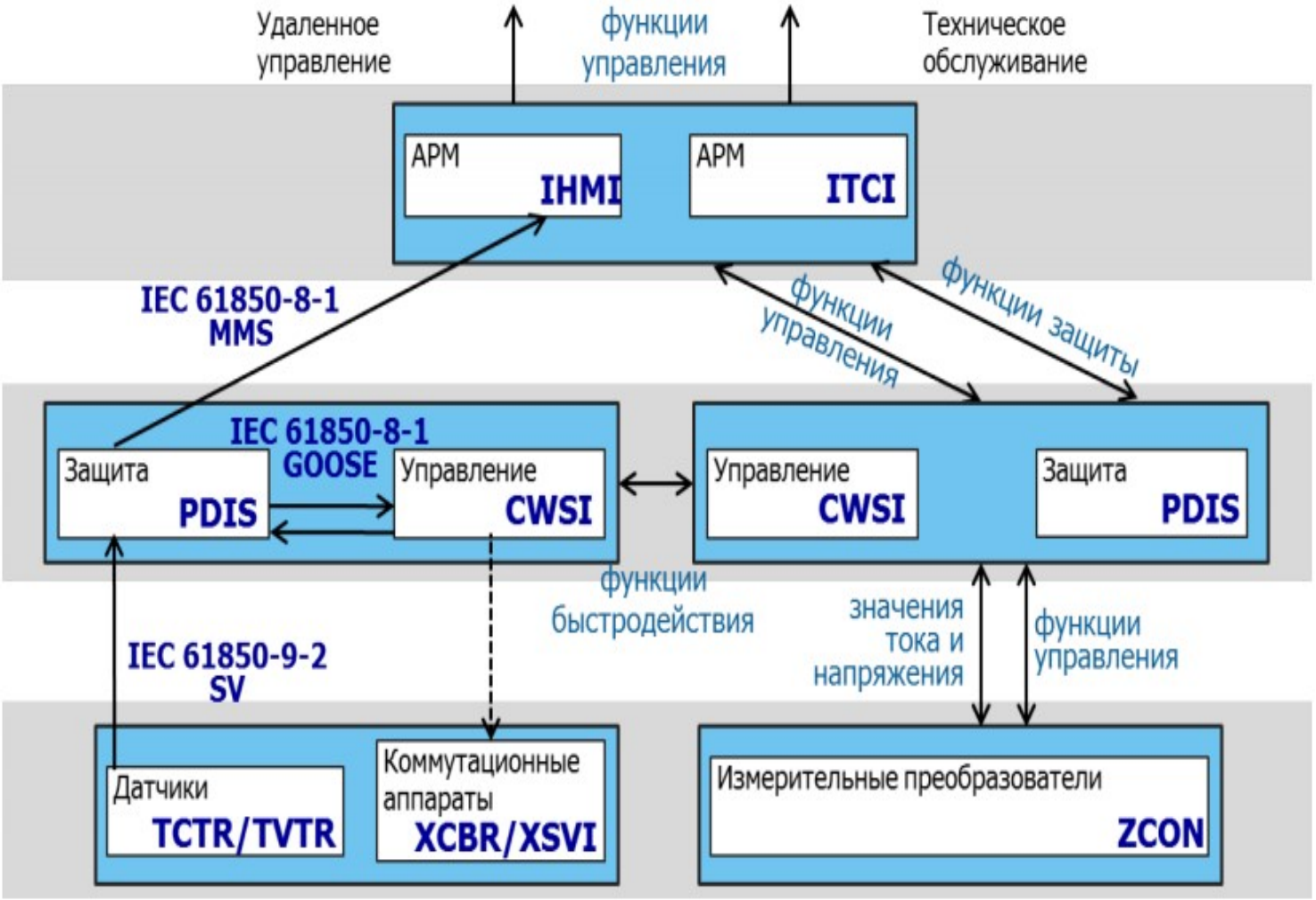
Використання перетворювачів для стикування різних стандартів і протоколів призводить до уповільнення роботи системи, підвищує ризик виникнення помилок, знижує надійність електропостачання.

Потрібен стандарт, щоб, з одного боку, захистити фінан-сові вкладення в енергетичне обладнання, з іншого – використовувати передові обчислювальні та комунікаційні технології.

Стандарт МЕК 61850
«Мережі та системи зв'язку на підстанціях»

Секція	Назва
МЕК 61850-1	Вступ і загальний огляд
МЕК 61850-2	Глосарій
МЕК 61850-3	Основні вимоги
МЕК 61850-4	Управління системою і проектуванням
МЕК 61850-5	Вимоги зв'язку до функцій і моделей пристроїв
МЕК 61850-6	Мова опису конфігурації зв'язку між мікропроцесорними електронними пристроями підстанцій
МЕК 61850-7	Основна структура зв'язку для обладнання підстанції та лінії живлення (4 частини)
МЕК 61850-8-1	Опис передачі даних по протоколу MMS
МЕК 61850-9-1	Вибіркові значення по послідовному ненаправленого багатоточковому каналу передачі даних типу точка-точка
МЕК 61850-9-2	Вибіркові значення по ISO / IEC 8802-3
МЕК 61850-10	Перевірка на сумісність

Інформаційна модель цифрової підстанції по МЕК-61850



Рівень станції

(Station Level)

Рівень з'єднань

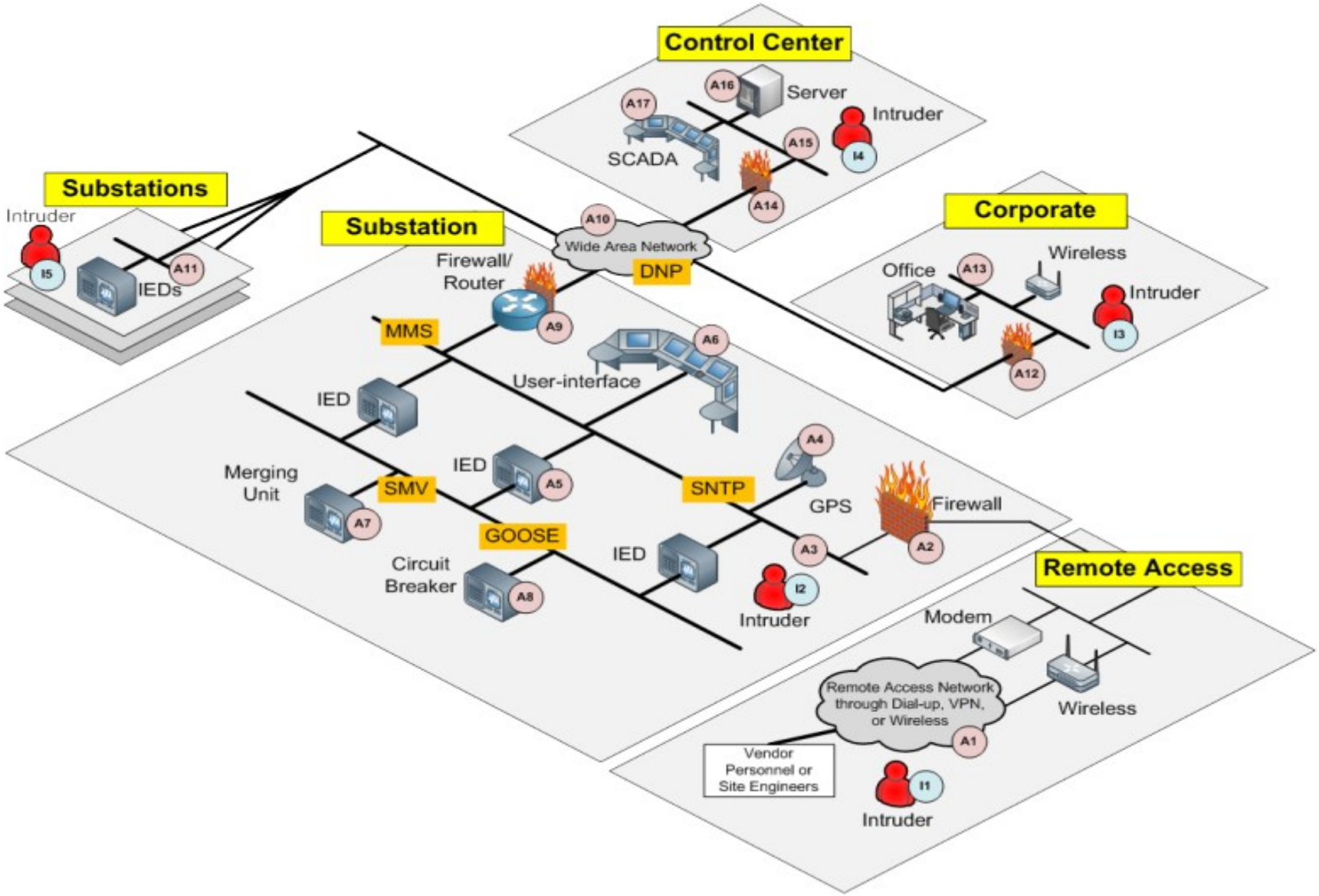
(Bay Level)

Рівень процесу

(Process Level)

(Field Level)

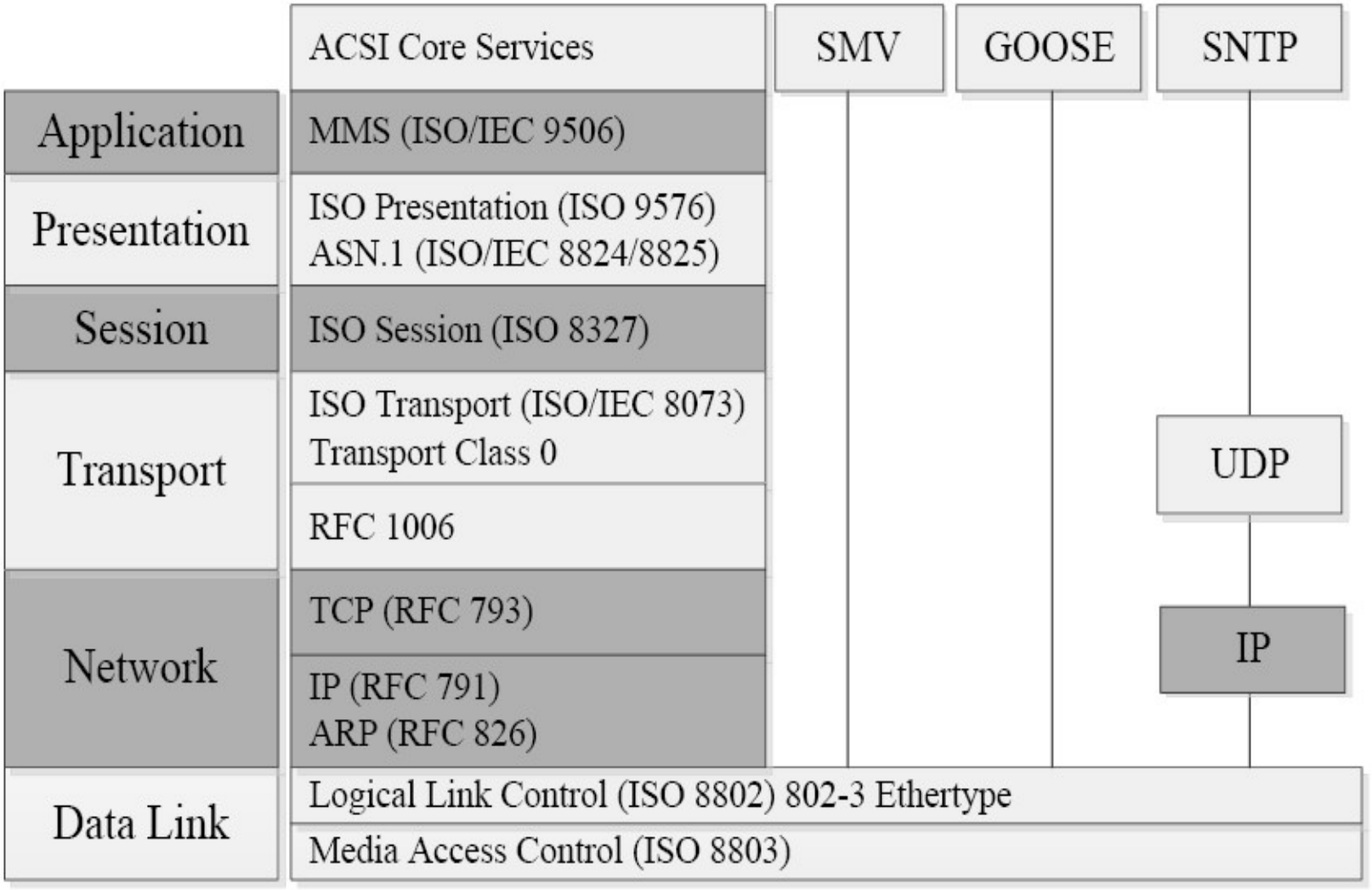
Загрози на підстанціях



Особливості кіберзахисту систем промислової автоматики

Якщо традиційні IT-комунікації є різнорідними і в широких межах варіюються за своєю природою, кіберфізичні системи мають певну сталу структуру і типові шаблони комунікації, які слід брати до уваги при виявленні підозрілої активності

Протоколи стандарту МЭК-61850



Особливості вразливостей протоколів МЕК 61580

Існує дев'ять основних шляхів використання вразливостей багатоадресних протоколів, до яких належать такі протоколи за стандартом МЕК 61580, як **GOOSE** та **SV**:

1) компрометація інтерфейсу користувача;
2) переривання процесу синхронізації часу;
3) компрометація шини зв'язку на станційному рівні;
4) отримання доступу до пристроїв рівня приєднання;
5) зміна налаштувань захисного пристрою;
6) захоплення та модифікація повідомлень протоколу GOOSE;
7) компрометація комунікаційної шини на рівні процесу;
8) розміщення підроблених значень у повідомленнях протоколу SV;
9) компрометація міжмережевого екрану для отримання доступу до мережі підстанції.

Мережеві системи виявлення вторгнень (МСВВ)

Глибока обробка пакетів

Системи виявлення вторгнень (СВВ)

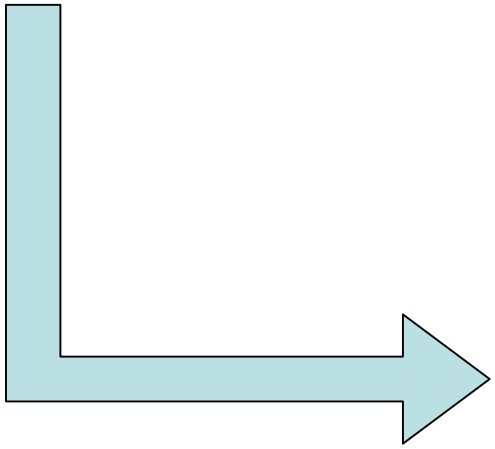
Классификация по методу анализа событий:

- Использующие **сигнатуры** (обнаружение злоупотреблений) – анализируют поток данных на соответствие сигнатурам – уникальным последовательностям, характеризующим конкретную атаку (**Signature**-based IDS - misuse detection)

- Выявляющие **аномалии** – необычное поведение пользователей, приложений или сетевых интерфейсов (Statistical **anomaly** based IDS)

Множинне розпізнавання рядків

... R o o T K I t + % 2 D + r o o t | 0 0 | 0 0 | ? C h e c k e r ...



"~root"

"root_path="

"root|00|"

"root|00|root|00|"

"/cgi-bin/cs.exe"

"/cgi-bin/cgsearch/search.cgi?"

"NetTracker"

"from=HL-Jacker"

Реконфігуровні обчислювачі

Традиційні реконфігуровні обчислювачі на базі ПЛІС, які застосовуються для апаратного прискорення в IT-сфері, розраховані на використання спільно з традиційними комп’ютерами, що ускладнює їх використання для захисту кіберфізичних систем

Можливості апаратного прискорення роботи СВВ на цифрових електричних підстанціях

1. Існують деякі технологічні задачі енергетики, для вирішення яких вже використовуються ресурси програмованої логіки, частину яких можна задіяти для цілей кібербезпеки, зокрема, для створення систем виявлення вторгнень. Прикладами таких застосувань можуть бути:

– системи управління, алгоритми яких засновані на використанні апаратів нейронних мереж і нечіткої логіки;

– інтелектуальні системи збору даних;

– частотні перетворювачі для керування потужними електроприводами тощо.

2. Інтелектуальні пристрої IED також мають в своєму складі ПЛІС або системи на кристалі для реалізації, зокрема, сумісних зі стандартом IEEE-1588 протоколів паралельного резервування з'єднань HSR (High-availability Seamless Redundancy) і PRP (Parallel Redundancy Protocol), а також для підтримки розглянутих вище протоколів стандарту МЕК 61850.

Параметри пристрою SMARTzynq Brick

Пристрій, розроблений для легкої інтеграції промислових мереж Ethernet в обладнання кіберфізичних систем

Пристрій містить:
• мікросхему класу "система на кристалі" (SoC) Xilinx ZC7020 Zynq;
• три-швидкісні інтерфейси Ethernet;
• ОЗП об'ємом 8 Гб на базі пам'яті DDR3;
• флеш-пам'ять на 256 Мб;
• ПЗП для зберігання унікального MAC-адреси;
• порти USB-UART, PMOD, мікро-SD
та ін.

У комплект поставки входять також IP-ядра інтелектуальної власності, що реалізують:
• протоколи HSR/PRP;
• індустріальний Ethernet;
• точну синхронізацію за стандартом IEEE 1588 для цифрових підстанцій.

Дякуємо за увагу!