UTeM
اونيۏرسيتي تيكنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 13

Always A Pioneer, Always Ahead

Resource Protection Requirements

Dr Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

OVERVIEW

- Introduction
  - What is the resources in the physical system?
  - What is the reason to protect the resources?
  - How to protect the resources?
- Resource Protection Requirement
  - Standard / Policy / Procedure / Framework / Guideline
  - Understanding Service Level Agreement (SLA)
- Conclusion

INTRODUCTION

What are the resources in the physical system or CPs?

- In the era of the industrial revolution, the current physical system has evolved through the use of internet-of-things for autonomous smart system in the cyber world.
- Cyber Physical System (CPs) integrates the physical system in the large scaled digital computer networked environment.
- The application of CPs spans in many disciplines, including agriculture, energy, medical, health care system, manufacturing, transportation, military and smart environment.
- The resources of CPs are hardware, software application, sensor, actuator, nodes and bring your own device (i.e: user's smartphone), which all assets are available inside the organization based on the discipline.

Example of resources

Discipline	Type of Asset	Name of the Asset and Description
Agricultural	Hardware	Drone – for fertilizer the plant
		Smart water management
Medical	System	electronic patient record initiative
Transportation	Hardware	cyber-physical vehicle system (CPVS) – sensor scheduling
Manufacturing	Service	Delivery of services

What is the reason to protect the resources for CPs?

- Since the cyber physical system (CPs) has been exposed to the internet, the crucial information has become available to others. The crucial information involve monetary values of assets, end products and other materials of the organization.
- Thus, the vulnerability in physical system infrastructure, create the opportunity for hackers to launch attacks.
- In fact, the IoT devices has lack of standard protocol and the platform is open for usage, which makes the potential loophole in protecting the resources in CPs.

How to Protect the Resources in CPs ?

- There are many ways to protect the resources in cyber physical system such as :
    - Standard / Policy / Procedure / Framework / Guideline
    - Understanding Service Level Agreement (SLA)
- Why need to protect the resources?
    - To achieve sustainability in ecosystem, human health and functions for future generation.

RESOURCE PROTECTION REQUIREMENTS

Standard / Policy / Procedure / Framework / Guideline

NIST FRAMEWORK

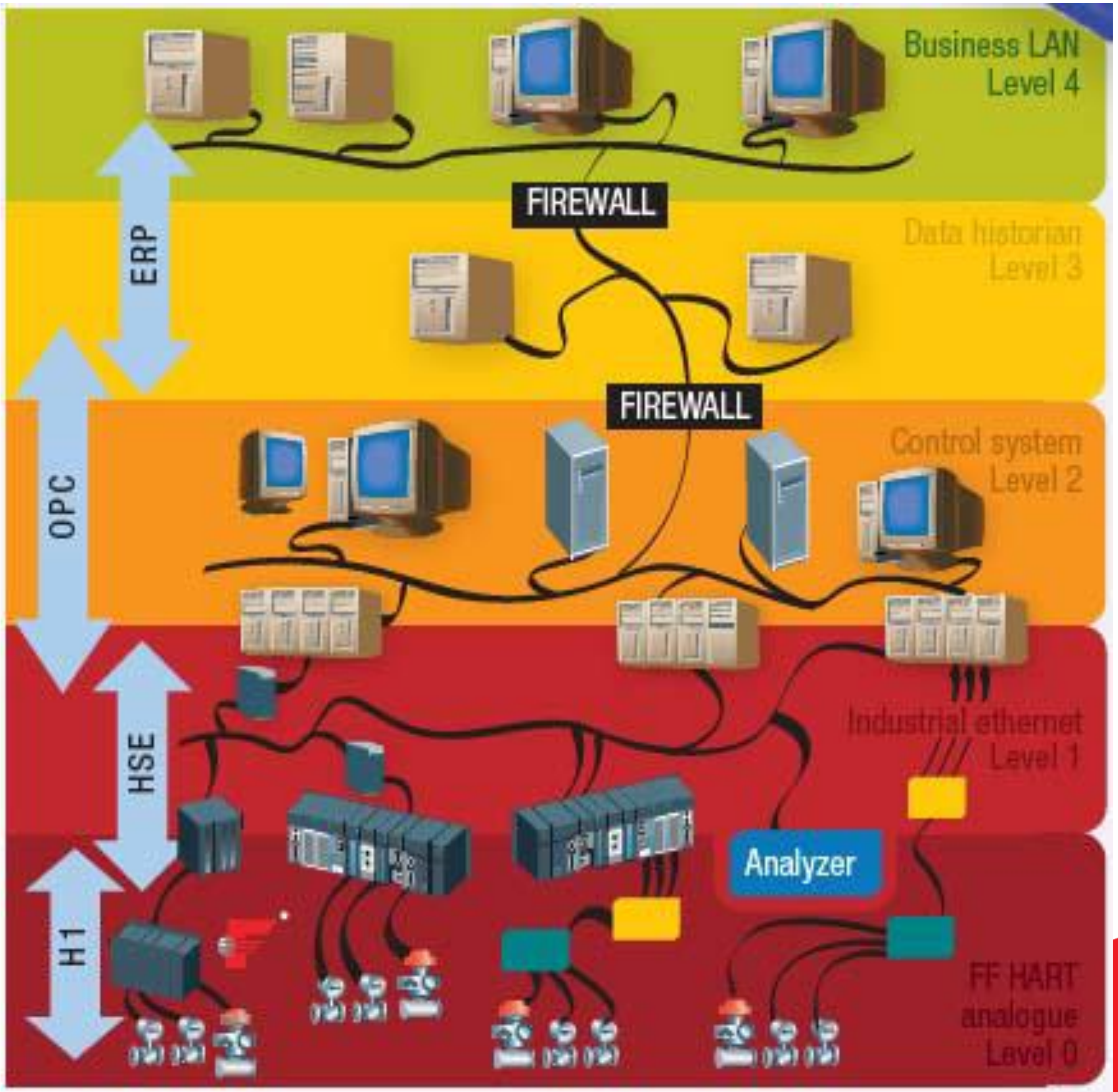
https://doi.org/10.6028/NIST.SP.1500-202

- The on-going development of standard through the integration between various similar standards services, provides understanding the scope of the problems address.
- The Metadata Access Points (IF-Map) uses the SOAP (developed by the OASIS Foundation) for data binding. REST is used for the binary protocols that interacts with web page exchange and utilizes the SSL/TLS security. The common transport protocol with security ISO/IEC/IEEE P21451-1-4 offers eXtensible Markup Language (XML) constructs known as IoT XEPs (Extensions) to the eXtensible Messaging and Presence Protocol (XMPP). This approach has security built into the protocol using Transport Layer Security (TLS) and makes use of trust engagement whereby all devices must be registered to participate in a network.

NIST FRAMEWORK

https://doi.org/10.6028/NIST.SP.1500-202

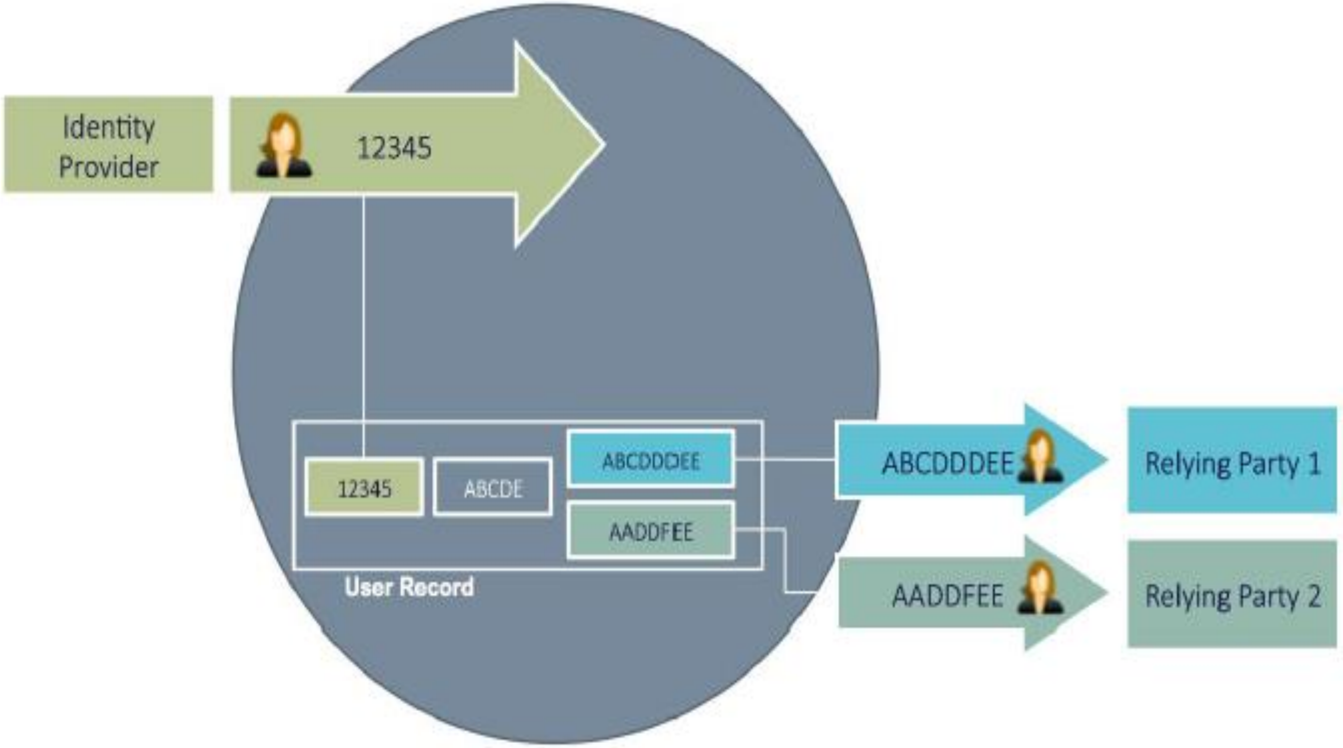
- Privacy has been another issue in conducting online transaction.
- In manufacturing for example, the topology design for protecting the resources in a chemical plant.
- The design shows that the equipment in the physical layers has been replaced with a better life long lifecycle for a replacement. Many of the offline sensors have been replaced with IoT sensor and adapt with the element of ubiquitous network technologies for a safe and better operations in the smart factory.



NIST FRAMEWORK

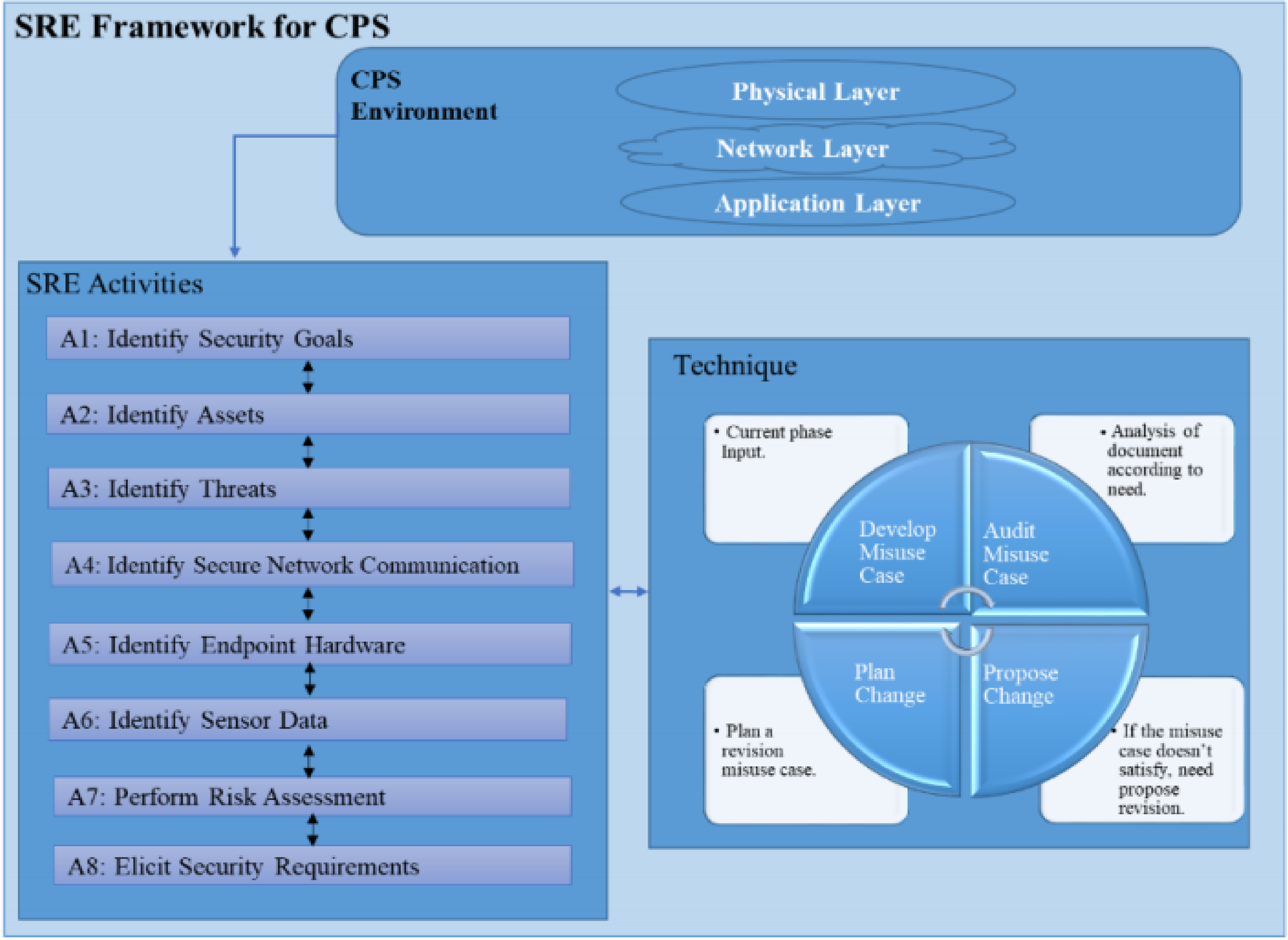
https://doi.org/10.6028/NIST.SP.1500-202

- The resource protection is under continuous refinement based on respective area, layers, protocols and domain of security.
- For example, to protect the password authentication of the employee, the design requirement is to ensure data privacy of the employee. The data privacy needs to be base on anonymity, unlikability and unobservability at the beginning of the design requirement.



The Double Blind Authentication

Shafiq ur Rehman and Volker Gruhn "An Effective Security Requirements Engineering Framework for Cyber-Physical Systems", technologies, MDPI, Vol 6(3), no. 65, pp: 1-20, 2018.



SRE Framework for CPS

CPS Environment

Physical Layer

Network Layer

Application Layer

SRE Activities

A1: Identify Security Goals

A2: Identify Assets

A3: Identify Threats

A4: Identify Secure Network Communication

A5: Identify Endpoint Hardware

A6: Identify Sensor Data

A7: Perform Risk Assessment

A8: Elicit Security Requirements

Technique

- Current phase Input.

- Analysis of document according to need.

Develop Misuse Case

Audit Misuse Case

Plan Change

Propose Change

- Plan a revision misuse case.

- If the misuse case doesn't satisfy, need propose revision.

- The framework recognizes the activities that an analyst needs to follow in order to identify the security requirements for CPs.
- The CPS framework has the following 8 activities (A1 to A8). These activities are selected based on their importance vis a vis security requirements and the characteristics of cyber-physical systems.

- A1 – Identify Security Goals
- A2 – Identify Assets
- A3 – Identify Threats
- A4 – Identify Secure Network Communication

A5 – Identify Endpoint Hardware

A6 – Identify Sensor Data Communication

A7 – Perform Risk Assessment

A8 – Elicit Security Requirements

Service Level Agreement (SLA)

SLA - 1

- An agreement between a business function owner and the service provider, which designates the amount of time, annualized basis, the business function will be available.
- SLA is associated with a business function, not with any particular machine, system or frame.

SLA - 2

- SLA should contain:
  - The list of services the provider will deliver and a complete definition of each service.
  - Metrics to determine whether the provider is delivering the service as promised
  - Auditing mechanism to monitor the service.
  - Responsibilities of the provider and the consumer
  - Remedies available to both provider and client if the terms of the SLA are not met.
  - A description of how the SLA will change over time.

SLA - 3

1. Security: Client and CPS must understand security requirements.
2. Data encryption: Data must be encrypted while it is in motion and while it is at rest. The details of the encryption algorithms and access control policies should be specified.
3. Privacy: Basic privacy concerns are addressed by requirements such as data encryption, retention, and deletion. An SLA should make it clear how the cloud provider isolates data and applications in a multi-tenant environment.
4. Data retention/deletion: How does CPS prove they comply with retention laws and deletion policies?
5. Hardware erasure/ destruction: Same as #4.
6. Regulatory compliance: If regulations must be enforced because of the type of data, CPS must be able to prove compliance.
7. Transparency: For critical data and applications CPS must be proactive in notifying client when the terms of the SLA are breached including infrastructure issues like outages and performance problems as well as security incidents.

SLA - 4

- Certification: CPS should be responsible for proving required certification and keeping it current.
- Performance definitions: Defining terminology such as uptime and other contractual metric terms (i.e. – uptime could mean all servers on continent are available or only one designated server is available.)
- Monitoring: Responsible party for monitoring including identification of any third-party organization designated to monitor performance of the provider.
- Audit Rights: To monitor for any data breaches including loss of data and availability issues. SLA should clarify when and how the audits will take place.
- Metrics: to be monitored in real-time and audited after occurrence. Metrics of an SLA must be objectively and unambiguously defined.
- Human interaction: On-demand self-service is one of the basic characteristics of cloud computing, but SLA should provide customer service when needed.

AGREEMENT CONSIDERATION

- Use of data/Security
- Location of data
- No change of terms
- Destruction
- Ownership (assignment)
- Subpoena response
- Regulatory requirements
- Insurance/Indemnity
- Audits

CONCLUSION

Conclusion

- In Cyber Physical System (CPs), the resources available in the system, requires protection for safety, sustainability and environmental friendly.
- The cyber law on protecting the resources in CPs is still a new study to be explored. Moreover, rules and procedures, legal act and standard for requirement resources protection are still in development and researcher needs to study for better framework.
- As for now, the requirements for resources protection is built based on the domain, area under study/problem, communication layers, protocols and technology available.

Thank You

MyUTeM

www.utem.edu.my