International Conference on ASEAN-JAPAN Cybersecurity Community

Trust Design for distributed Energy Resource Aggregation System on Cyber and Physical Security Framework”

October 2023

Project Leader, Systems Committee on Smart Energy, IEC
Keio University, Japan
Masaki Umejima, Ph.D
Director, National Advanced IPv6 Center (NAv6)
Universiti Sains Malaysia
Selvakumar Manickam, Ph.D

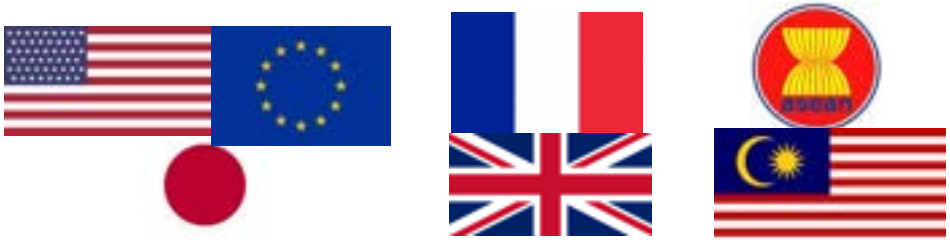
IEC System Committee Smart Energy

- The International Electrotechnical Commission（IEC）is a global non-profit organization that provides 10,000+ international standards, gathering 20,000 experts in more than 170 countries.
  - **System Committee Smart Energy（SyC SE）in IEC provides systems-level standardization for smart energy and smart grids.**

Cyber Civilization Research Center（CCRC）, Keio University

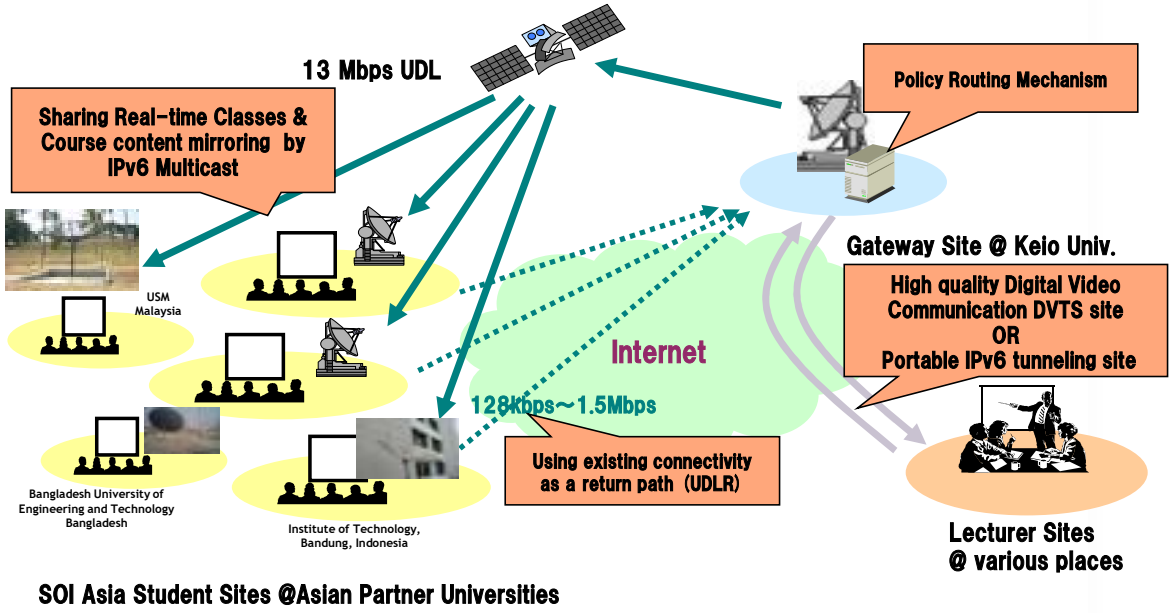
- *CCRC is addressing the security design of cyber and physical space with the leadership by the Internet giants in U.S. and Japan.*
- *Trust design of Cyber-Physical system like Energy Resource Aggregation Business system is our research interest. So, CCRC has done its related research, partnering with the institutions in U.S., EU, and ASEAN,*

Dr. David Farber:Left
the **Internet** Hall of Fame
Fellow, the American Association for the Advancement of Science〔AAAS〕
Dr. Jun Murai:Right
the **Internet** Hall of Fame
Special Advisor to the Cabinet

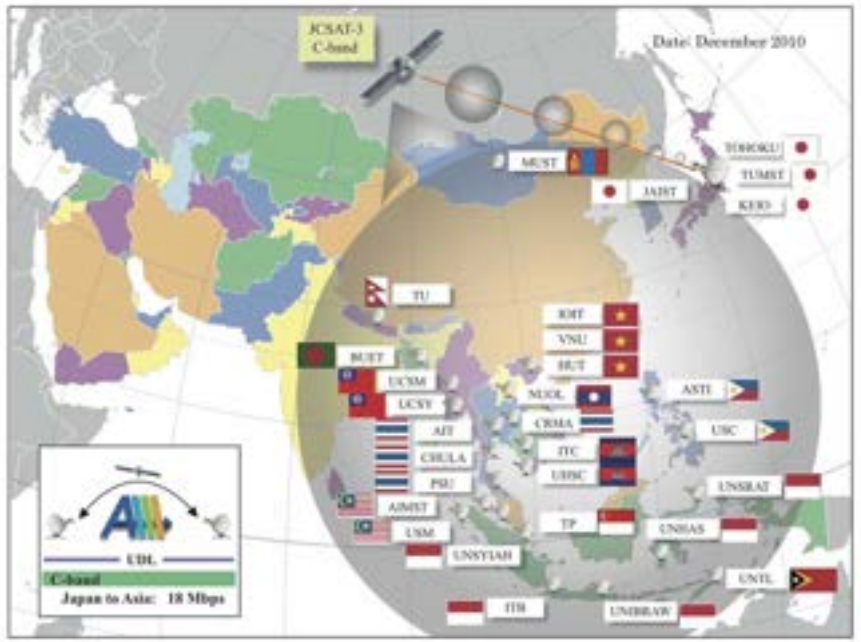


SOI Asia platform

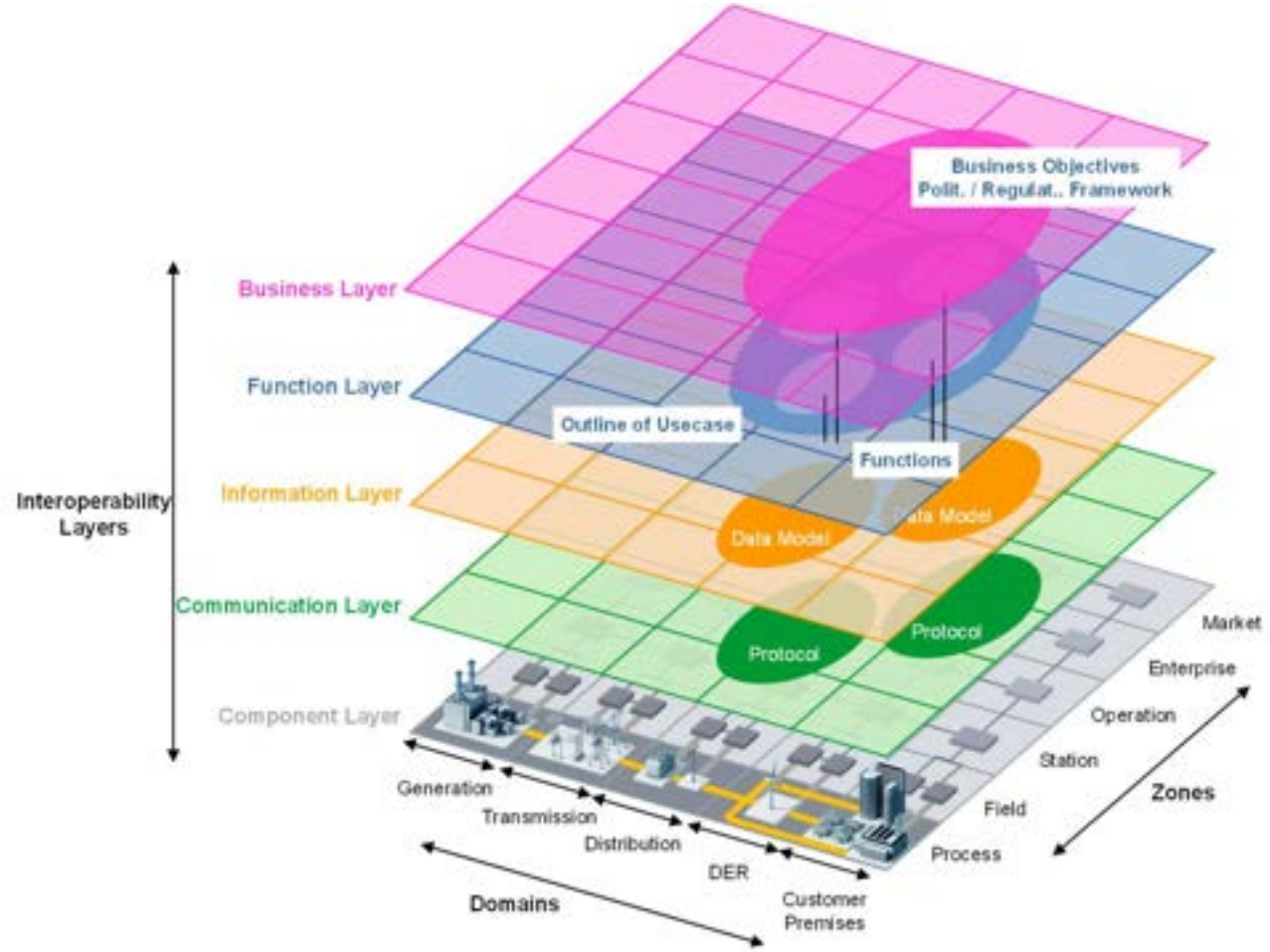
- SOI Asia is the university alliance, connecting leading Asian-wide universities by the high-speed network configuring satellite communication and the internet.
  - Dr. Jun Murai, the father of the internet, has addressed SOI Asia in 1996 that is one year after when the internet was commercialized.



SOI Asia Student Sites @Asian Partner Universities

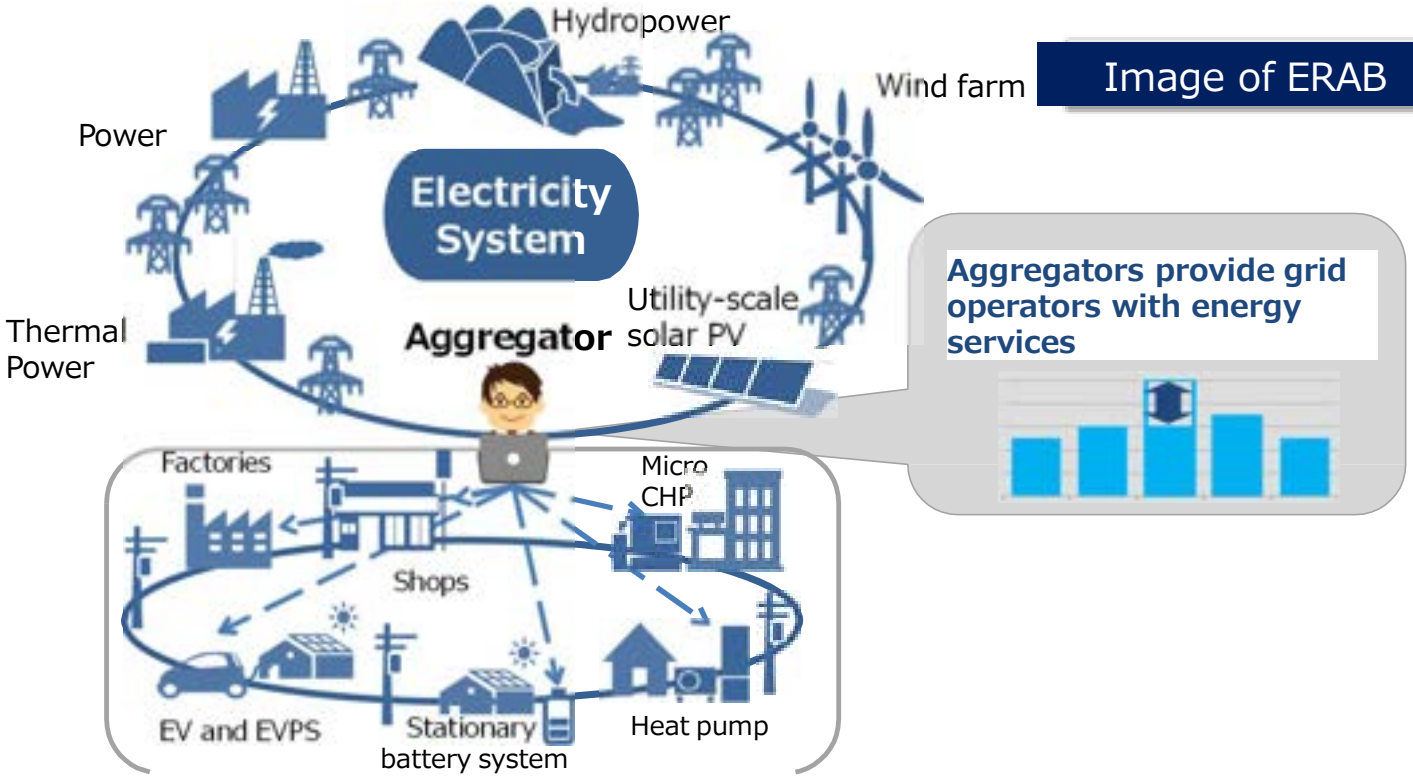


SGAM Plane by ”SMART GRID STANDARDIZATION ROADMAP” by SRD63097 in IEC SyC



ERAB enables the new relation between People and Energy

- Energy Resource Aggregation Business (ERAB) is a new business framework controlling distributed energy resources at a demand side like EV, a station battery, a fuel cell, and an air conditioner.



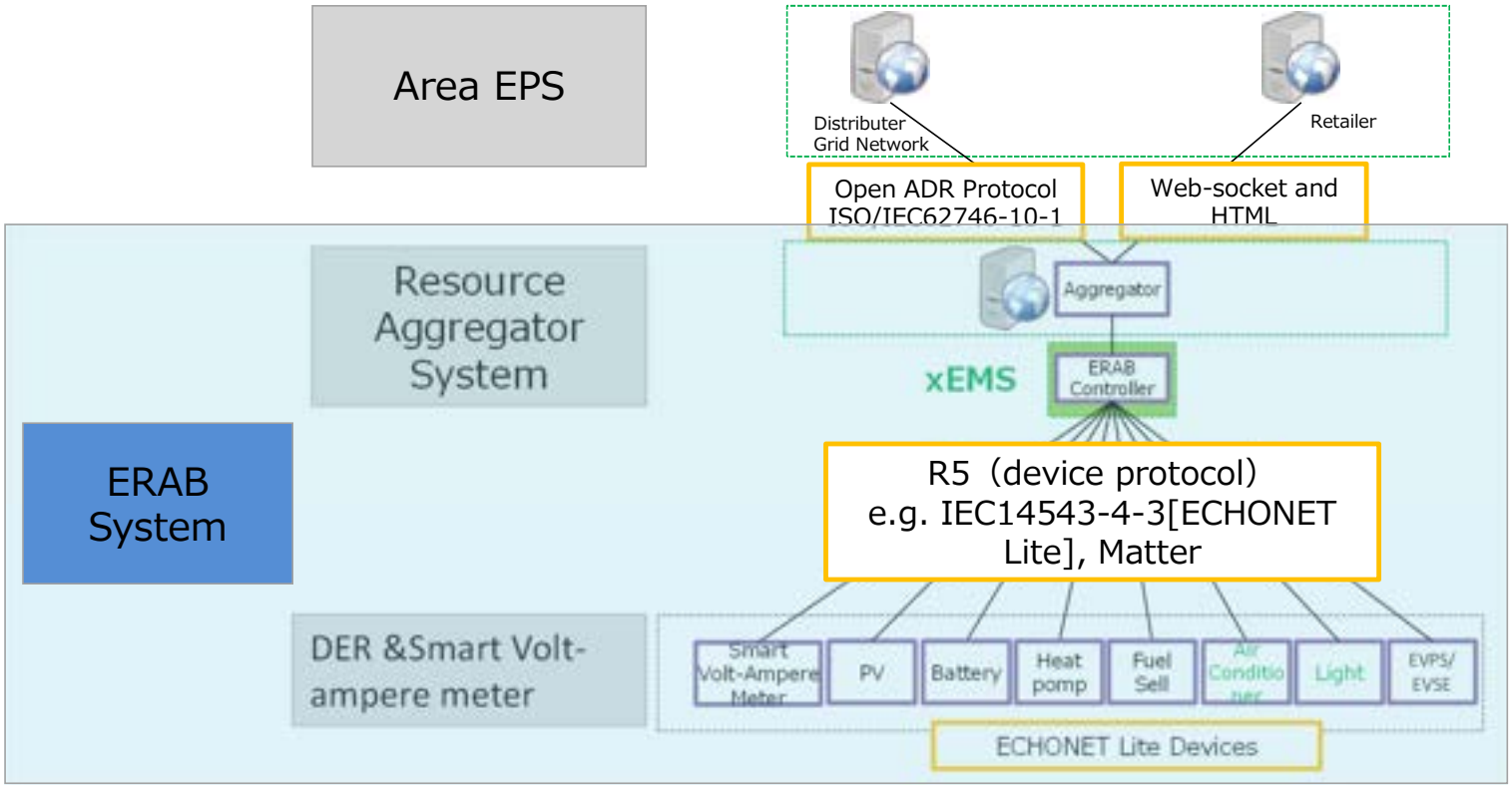
- The system is to **restrain or elevate the demand according to the request by retailers and a grid distributor** and to **provide the electricity traded in a supply and a demand adjustment market.**

6

Companies that have entered or shown interests in ERAB in Japan

Sample of ERAB system: remotely control DERs at a customer premise

- DER is a small-scale power generation source, located close to where electricity is used (e.g., homes or businesses), have the potential to provide an alternative to the traditional electric power grid.




IoT-Gateway [EMS Controller]


Light & Air conditioning


PV

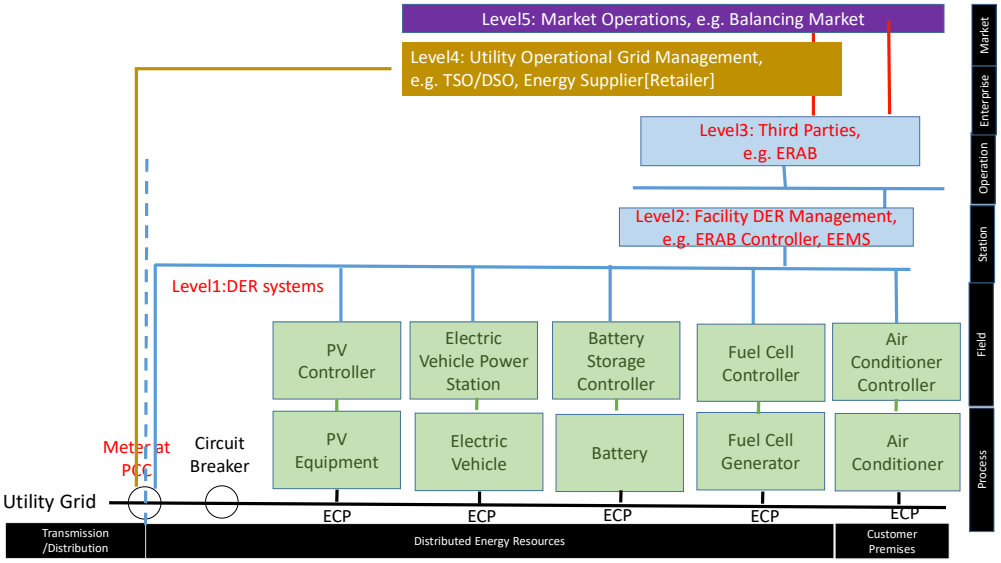
Activity towards SRD 63443: in SyC-SE

Title : Distributed Energy Resource Aggregation Business System: Architecture and Service scenario

The decentralized generation of electrical power as well as spread of energy storage and controllable loads becomes more and more important. The management of these Distributed Energy Resources［DERs］and Controllable Loads［CLs］at the customer premise near to the final customer offers economic and ecological benefits. In addition, information of Advanced Metering Infrastructure［AMI］provides a customer with the method measuring the value of aggregating these resources.

This activity aims to describe a distributed Energy Resource Aggregation Business（ERAB）in spotlighting a business & function layer on SGAM in SRD63097. Currently, we defined ERAB as:

Energy Resource Aggregation Business［ERAB］restrain or elevate power generations of DERs and demands of CLs in accordance to the performance measurement by the information of AMI and the requests by TSO/DSO, Electricity Supplier, and Energy Exchange.

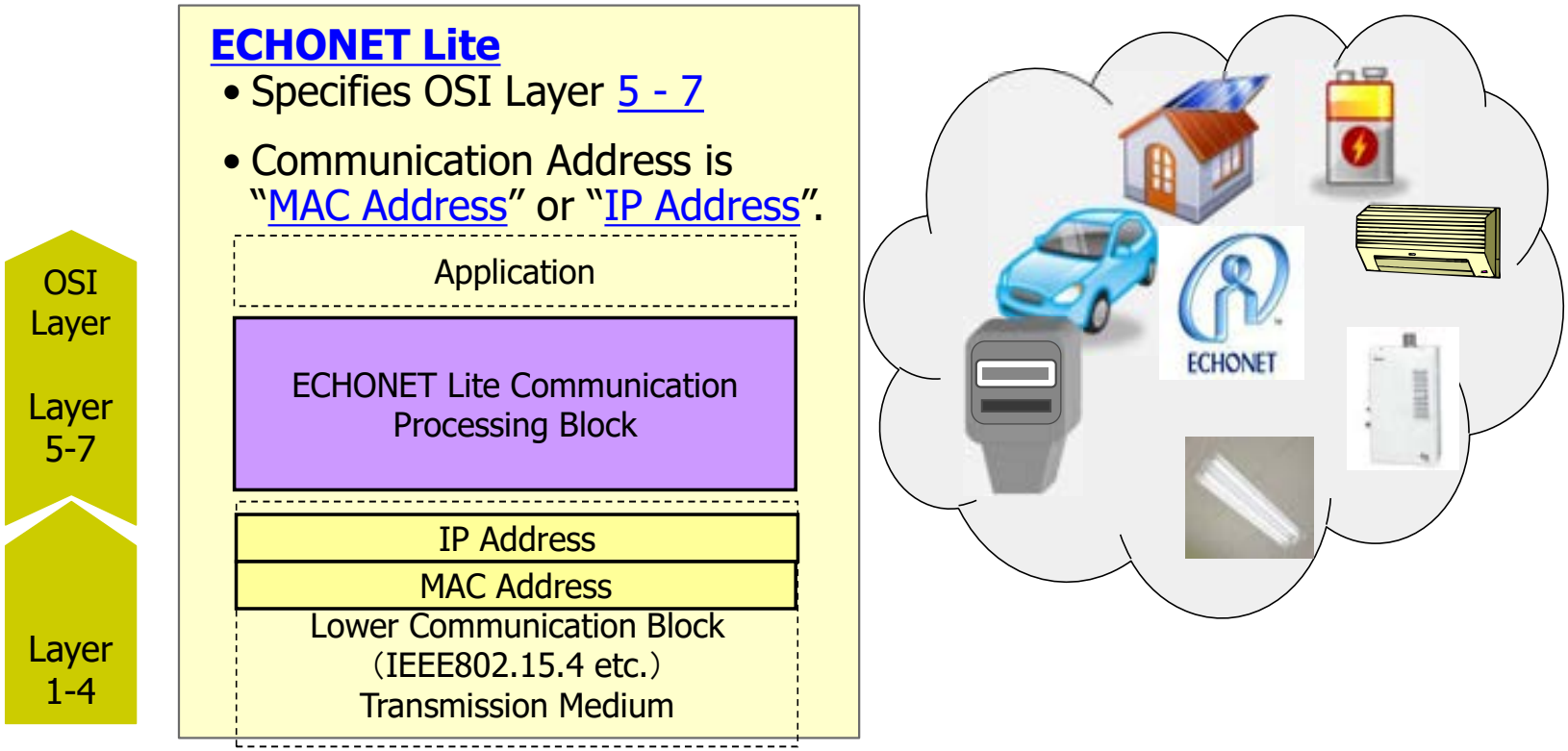


ERAB case is compatible with BUCs shown at IEC TR 63097:2017 SMART GRID STANDARDIZATION ROADMAP

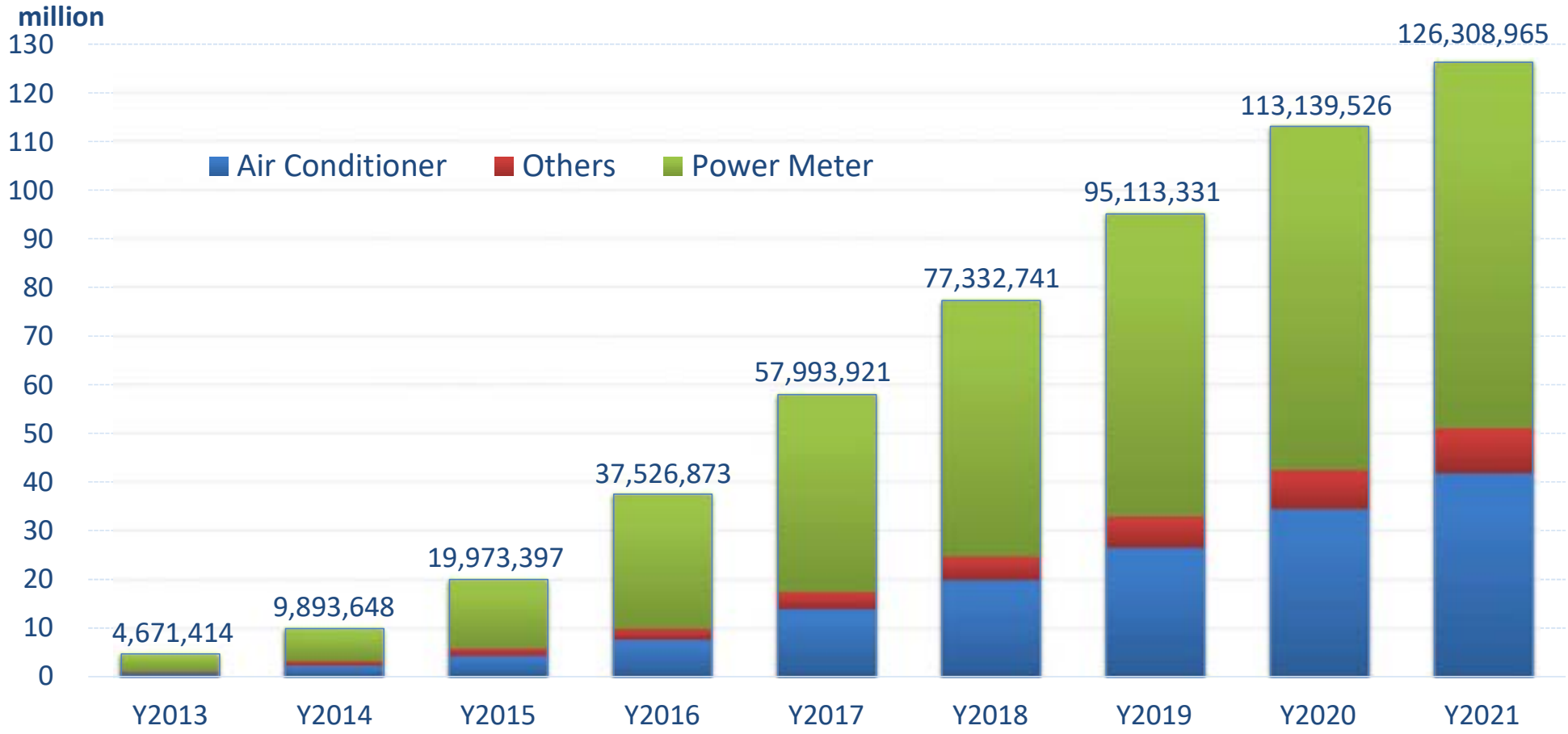
Project Leader: JP
With experts from France, Canada, U.S. India, Korea, Australia

Standardization giving to DER interface at a customer premise
It reduces the cost of configuring multiple DERs

A current condition in Japan surrounding ERAB system is that DERs speak a single language called ECHONET Lite. Japanese Government and Industry liaison has proposed ISO/IEC14543-4-3, to be the enabler of the demand side management, around HEMS. Internet of Things over this international standard, ECHONET Lite in Japan, has provided a common language for 100s of devices: home appliances, power meter, EV, and PV



ECHONET Lite devices: Approx. 138 millions in 2022



Lineup of DERs with ECHONET Lite

- In general, 30-40 Kw electricity is necessary for running a grocery store.
  - Lawson at SFC has the 12Kw solar power generation on the roof and the 5.6 Kw EV battery charger outside, connecting with EV which carries over 50Kwh battery.

※DER=Distributed Energy Resources

5.6 kw for storage

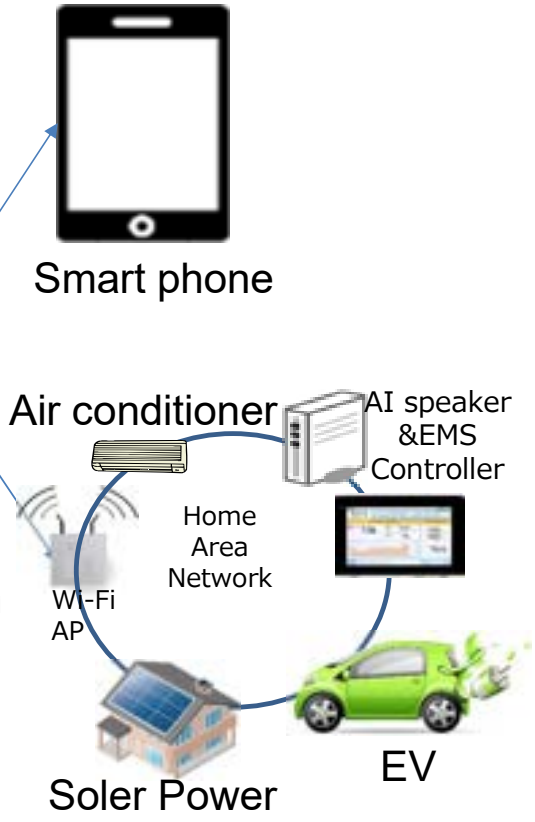
12 kw for generation

30-40 kw for usage
such as Air Conditioning

Next-gen power meter released in 2025

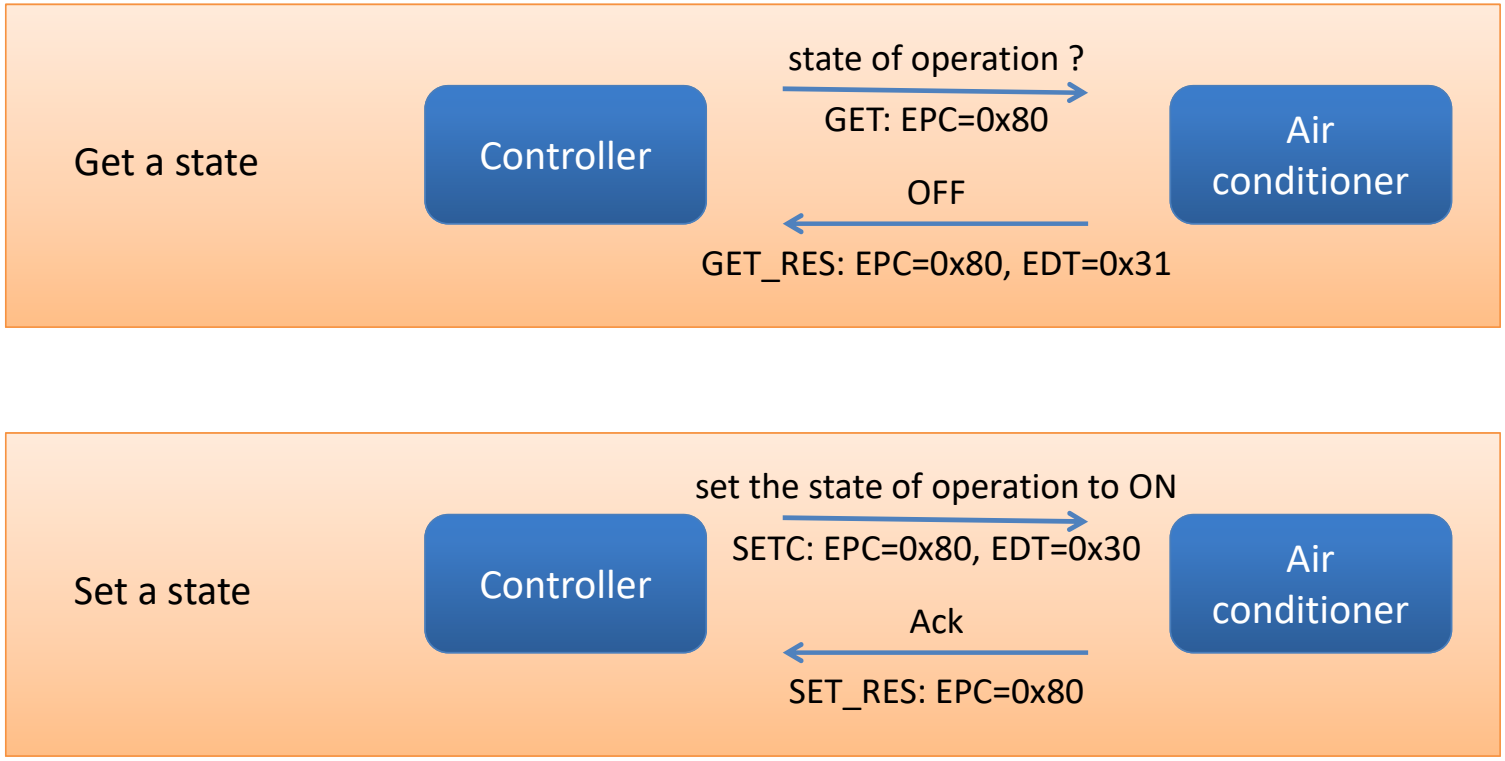
- Everyone's Mob App can access the electricity usage data: The ambitious nationwide project starting in 2025 in Japan

In 2025, a smart electricity meter in Japan starts to speak a common language over IPv6 on WI-Fi.



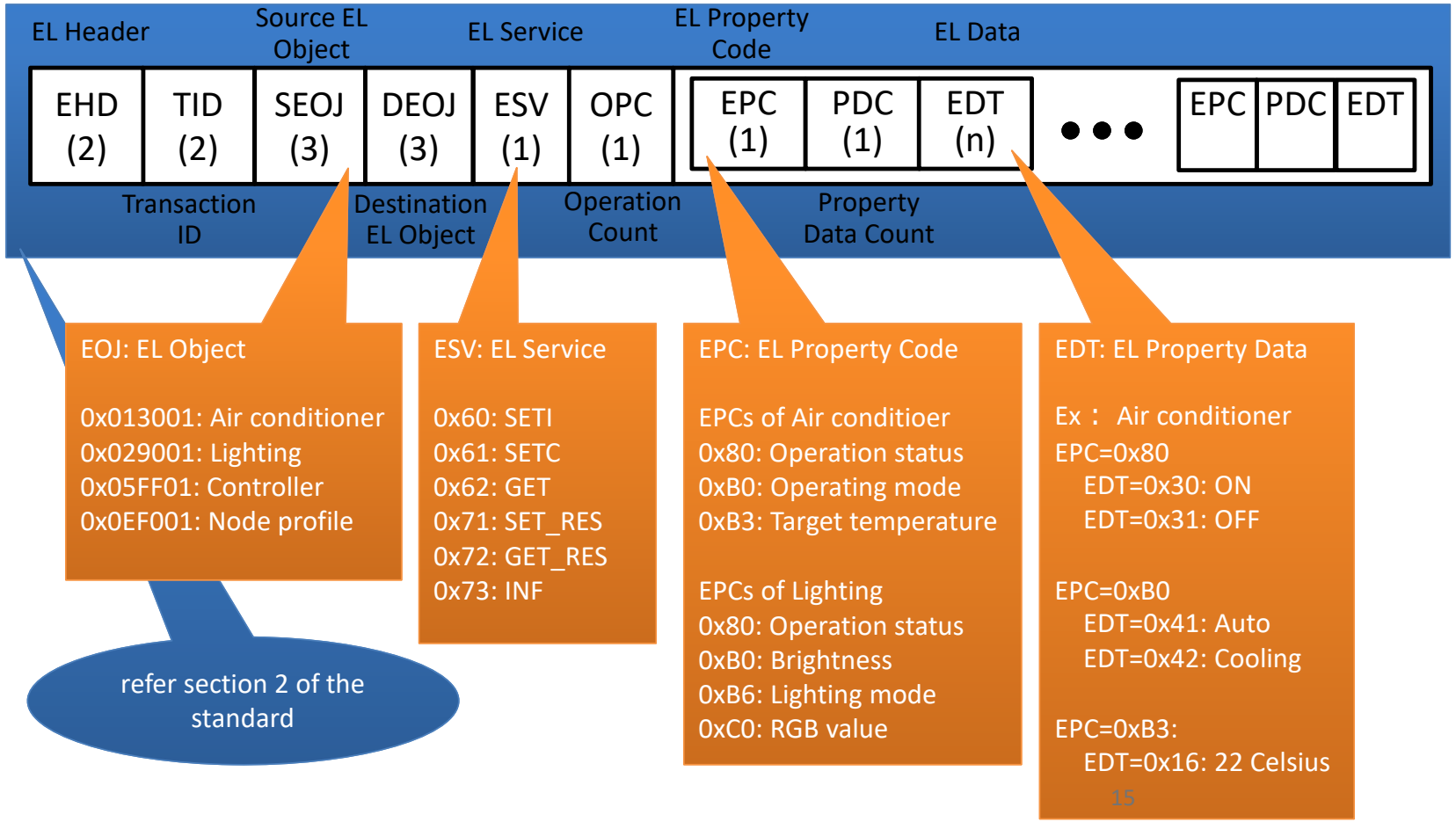
- The Japanese smart meter has two interfaces; B-root connects the meter with a user-owned device, complying with ECHONET Lite over an IPv6 single stack. A-root connects the meter with the utility company.
- New meter speaks a common language over IPv6 Link Local Address on Wi-Fi and Ethernet, covering nationwide users which is Approx. 90 millions

ECHONET Lite communication



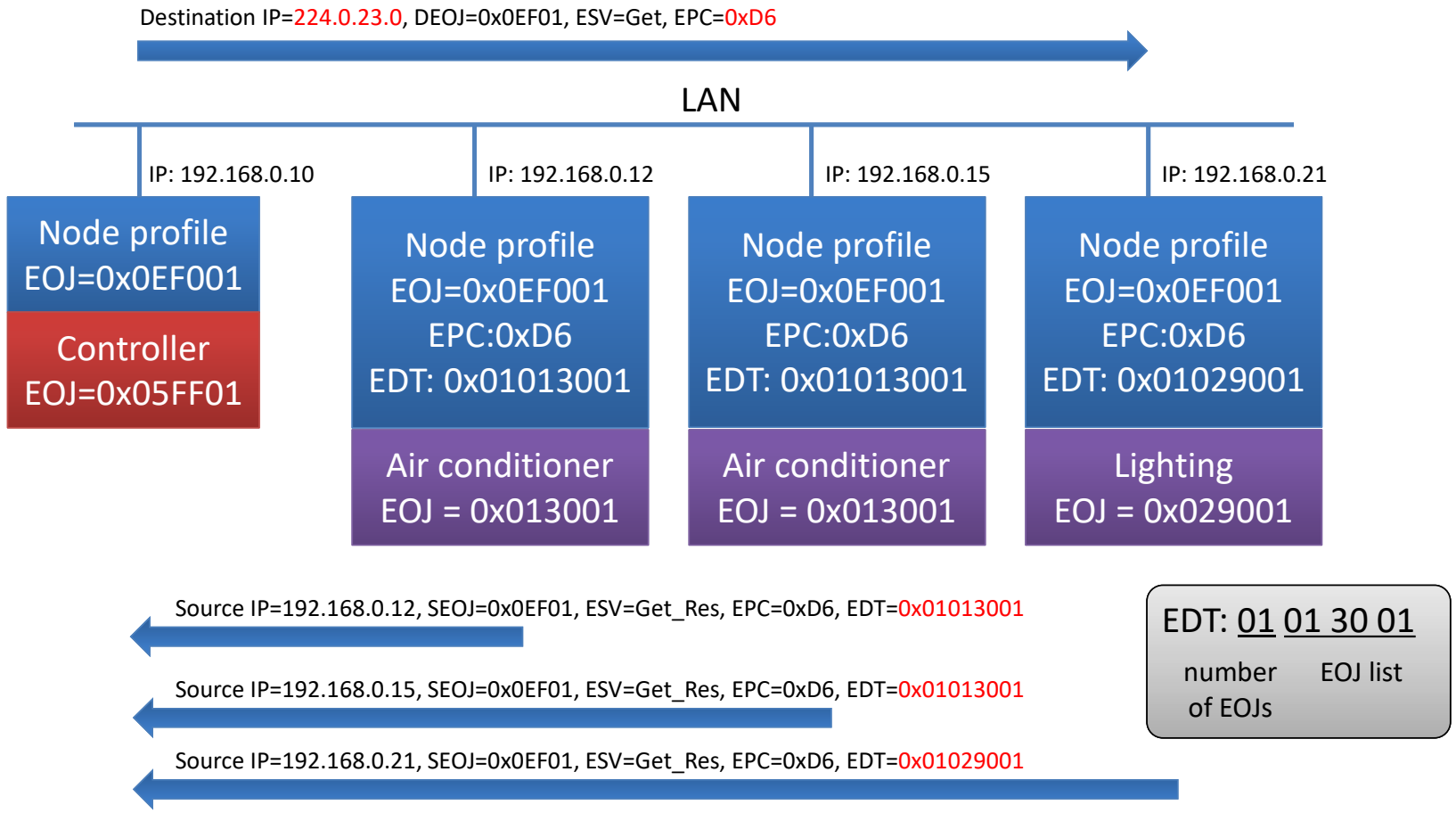
- UDP, Port 3610
  - Multicast address: 224.0.23.0
- Basic commands: GET, SET and INF
  - GET: Get property value
  - SET: Set property value
  - INF: Inform property value
- Every item is defined by binary data

ECHONET Lite Data Frame



Device discovery on ECHONET Lite

A controller searches ECHONET Lite devices



Node profile EPC=0xD6: instance list S

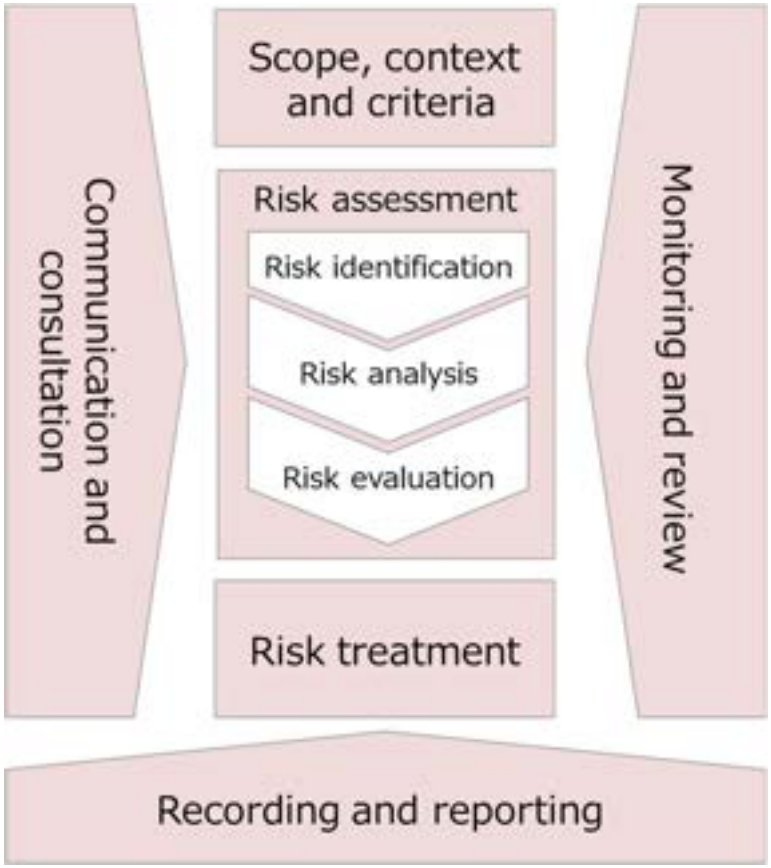
Examples of communication protocols for Distributed Energy Resources

- Matter will enable communication across smart home devices, mobile app, and cloud services, and define a specific set of IP-based networking technologies for device certification.
- CSA in charge of Matter is the standard body for inter-connected devices created by the formerly Zigbee alliance. The membership has covered with: Amazon, Apple, COMCAST, Google, Huawei, IKEA, and so on

- Japanese Government and Industry liaison has proposed ISO/IEC14543-4-3, to be the enabler of the demand side management, around HEMS. Internet of Things over this international standard, ECHONET Lite in Japan, has provided a common language for 100s of devices: home appliances, power meter, EV, and PV.

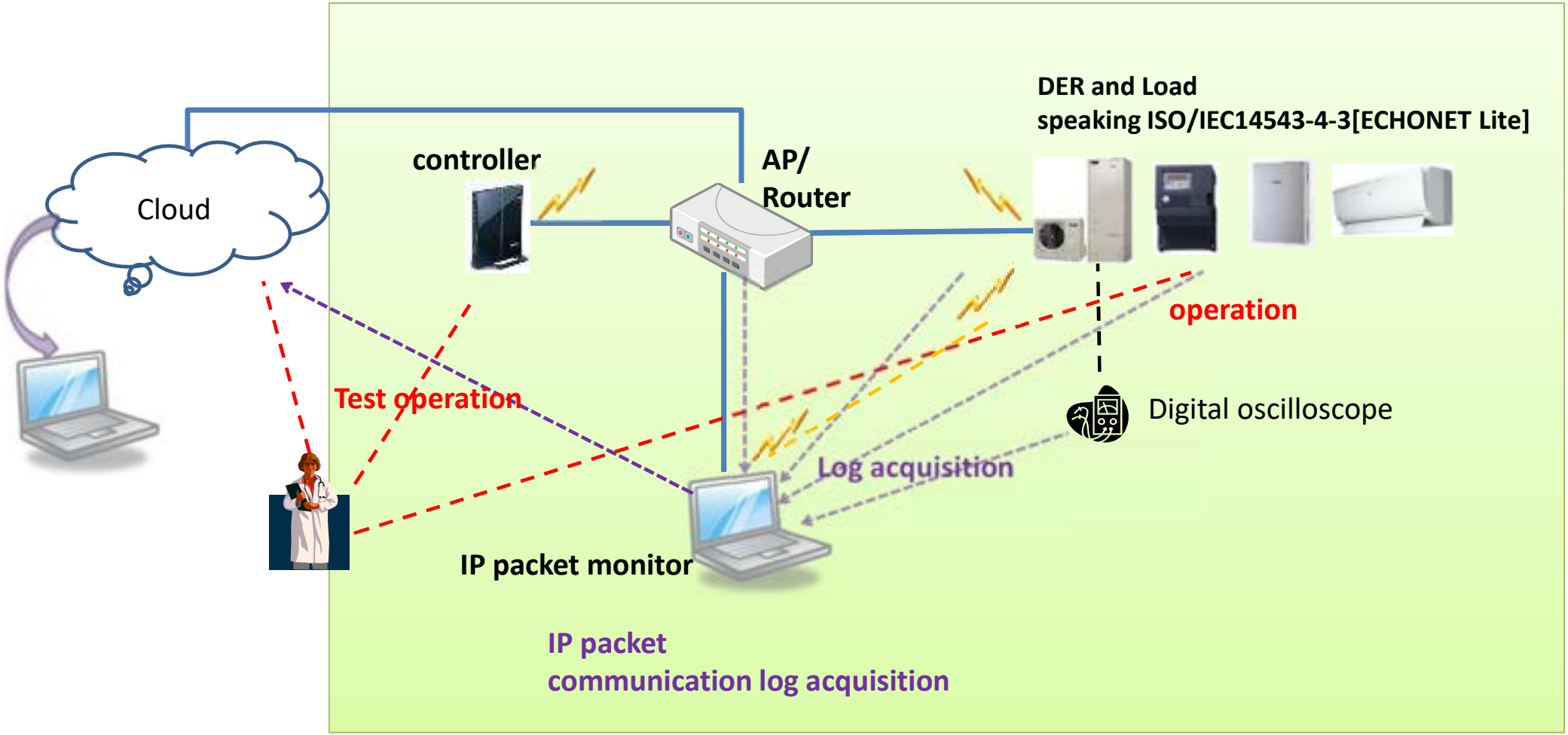
Proceed with risk management

- Ppoceed with risk management that considers three-layer model and six elements in CPSF, citing ISO 31000:2018 and ISO/IEC 27001:2013.



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

A penetration test-bed on the common network design at a customer premise



National Advanced IPv6 Centre

Universiti Sains Malaysia

A Brief Introduction

Background


NAv6
National Advanced IPv6
Centre of Excellence
USM
UNIVERSITI SAINS MALAYSIA
NAv6
NETWORK
RESEARCH GROUP
1992 - Network Research Group (NRG)
2005 - National Advanced IPv6 Centre of Excellence (NAv6) in Malaysia to implement IPv6 agenda
2008 - National Advanced IPv6 Centre (NAv6) as a center of excellence under the Senate USM.

R&D Areas

High Impact Publication •
Cutting Edge Experiments •
Local & International Grants •
Local & International Collaboration •
Experimental Campus Testbed •

• Training/certification Programs
• Contract-out Services
• Work with commercialization arm

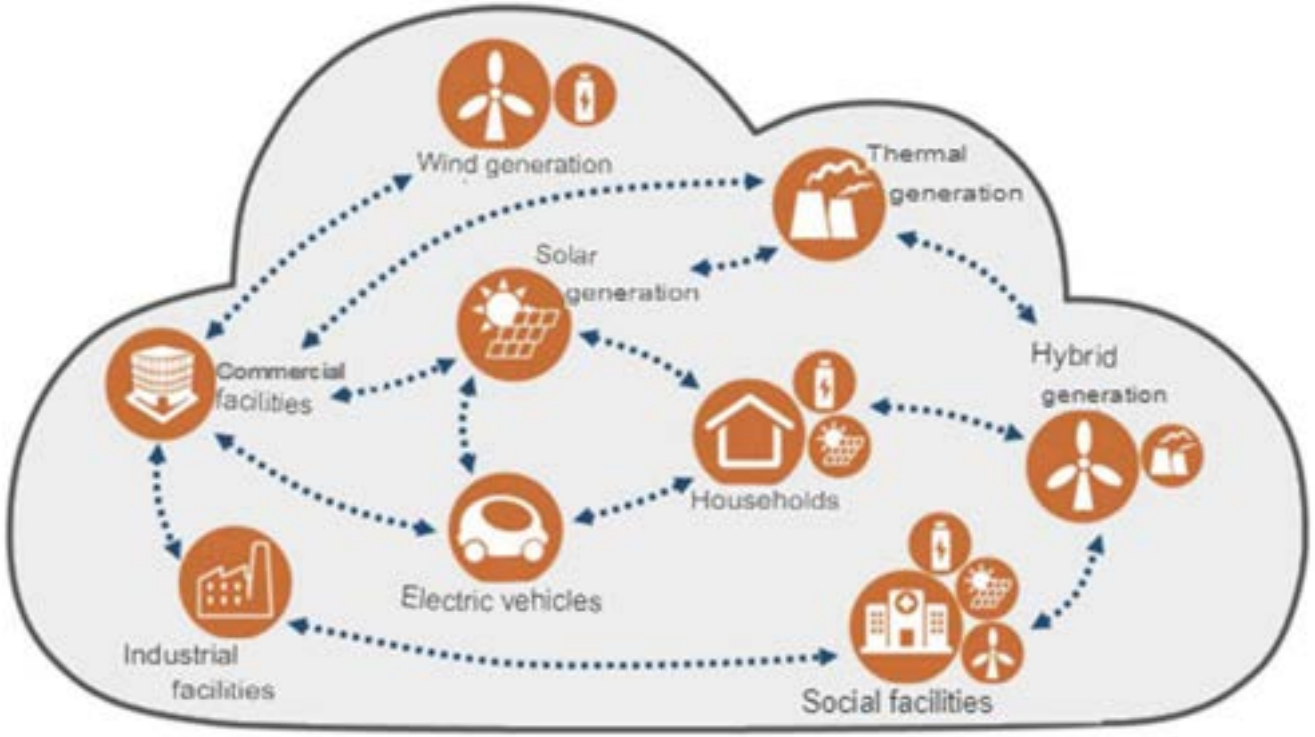
MSc and PhD Supervision •
MSc Cybersecurity •
Short Courses on Emerging Tech •

• Local & International Internship
• Staff Exchange Program
• Industrial Collaboration
• Community Outreach Programs

Focus Areas


Augmented Reality
Cloud Computing
Wireless Communication
Machine Learning
Internet Protocol
Software Defined Network
IPv6
Virtual Reality
Fog Computing
Industry 4.0
Data Science
Artificial Intelligence
M2M and V2V
Internet Governance
Embedded System
Cyber Security
Web Technologies
Drone
Cyber-Physical System
Smart Objects
Sensor Network
Robotic Process Automation
5G
Data Analytics
Blockchain
Internet of Things
Mobile Communication
Edge Computing
Mobile Application
Satellite Communication

Digitalization of DER Ecosystem

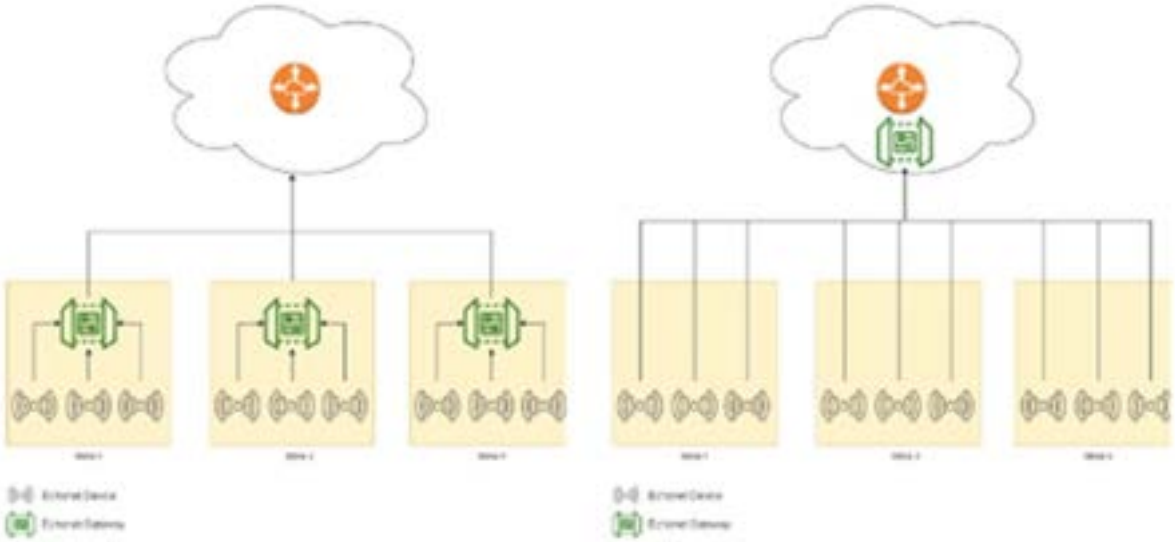


Digitalization of DER Ecosystem

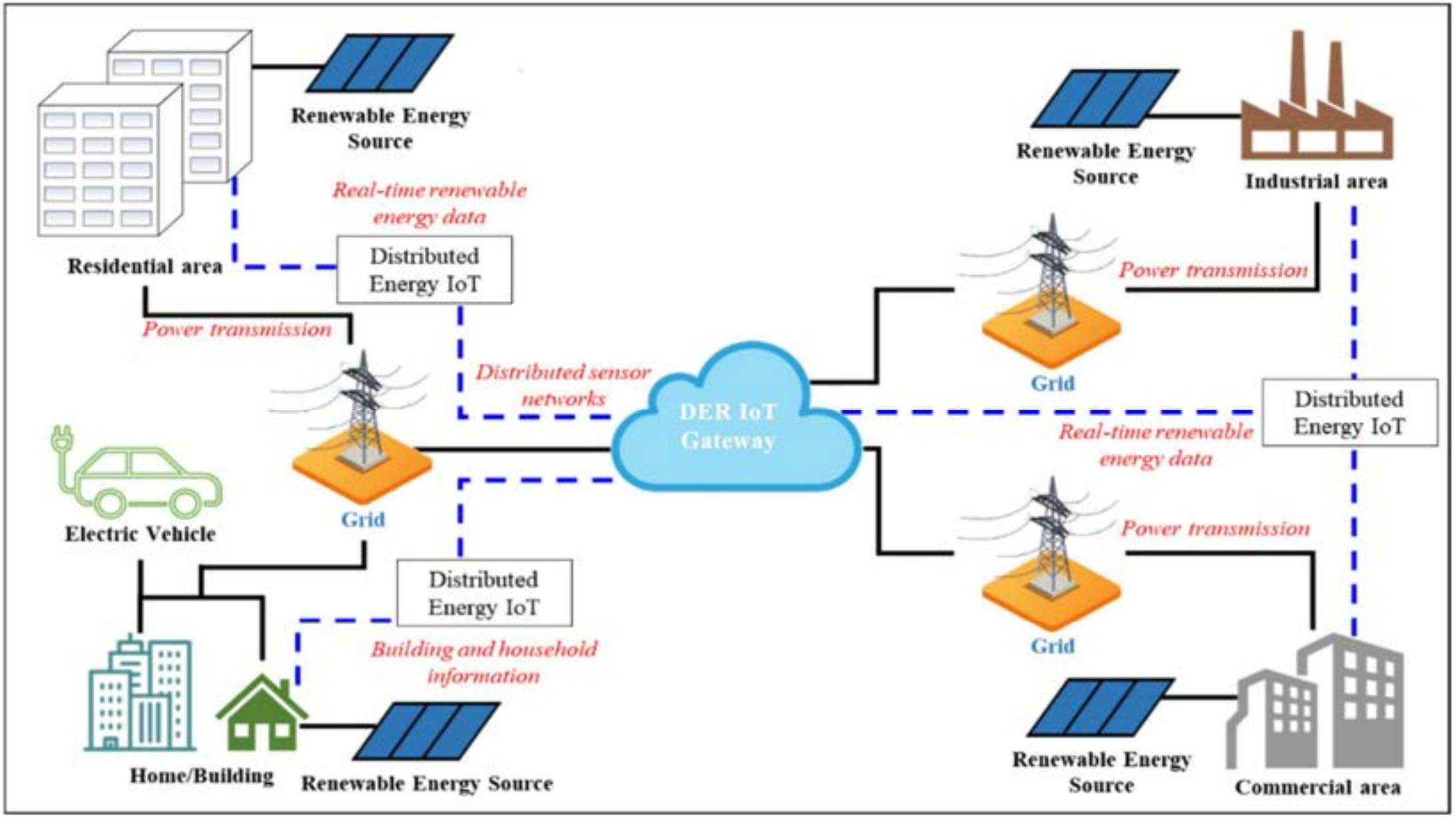
- **Increased Visibility and Control**: Digitalization offers real-time visibility, aiding DER owners in better asset management and optimization.
- **Improved Efficiency**: Digital tools automate tasks like scheduling and maintenance, enhancing operational efficiency for DER owners.
- **New Revenue Opportunities**: Digitalization opens avenues for generating revenue through grid services like frequency regulation and voltage support using DERs.
- **Reduced Costs**: Digital tools optimize energy consumption and cut waste, leading to cost reductions for DER owners.
- **Enhanced Customer Experience**: Digitalization allows for more customer interaction, offering real-time insights into energy usage and personalized energy management services.

IOT Gateway: a controller to facilitate DERs

- A DER gateway system, like an IoT gateway, collects and aggregates data from various DERs.
- The gateway bridges communication between DERs, IoT devices, sensors, other equipment and the cloud. By systematically connecting the field and the cloud, the gateway offers local processing and storage capabilities as well as the ability to autonomously control DERs based on data sensor input.



a Physical IoT GW (left), b Cloud-based IoT GW (right)


Renewable Energy Source
Real-time renewable energy data
Residential area
Distributed Energy IoT
Power transmission
Distributed sensor networks
DER IoT Gateway
Grid
Electric Vehicle
Distributed Energy IoT
Building and household information
Home/Building
Renewable Energy Source
Renewable Energy Source
Industrial area
Power transmission
Grid
Distributed Energy IoT
Real-time renewable energy data
Power transmission
Grid
Renewable Energy Source
Commercial area

Physical On-Premise Gateway

Advantages

- **Low latency**: **Data processed locally, reducing latency for critical applications.**
- **Privacy and data control**: **Data stays within organization's infrastructure, providing greater control and compliance.**
- **Reliability**: **Can continue to function without Internet or cloud service disruption.**
- **Scalability**: **Can be scaled to meet specific needs without relying on cloud resources.**
- **Security**: **Additional layer of security as data doesn't travel over public Internet.**
- **Cost-effectiveness**: **Cost-effective for large-scale deployments as reduces data transmission costs.**

Disadvantages

- Limited processing power: May not be able to handle complex analytics.
- Maintenance overhead: Organizations responsible for maintaining and updating hardware and software.
- Initial setup: More complex than cloud-based solutions.
- Scaling challenges: Can be difficult to scale as IoT ecosystem grows.
- Single point of failure: If gateway fails, entire IoT system may be disrupted.
- Limited remote access: Access to data and control may be restricted.
- Cost of ownership: Higher initial hardware and ongoing maintenance costs than cloud-based alternatives.

Security Advantages

1. **Centralized Security Management**: DER gateways centralize security management, simplifying policy implementation and enforcement.
2. **Enhanced Visibility**: They offer improved visibility into the DER system, enabling faster detection and response to security incidents.
3. **Comprehensive Security Features**: DER gateways include authentication, authorization, encryption, and intrusion detection, fortifying the DER system against unauthorized access and cyberattacks.

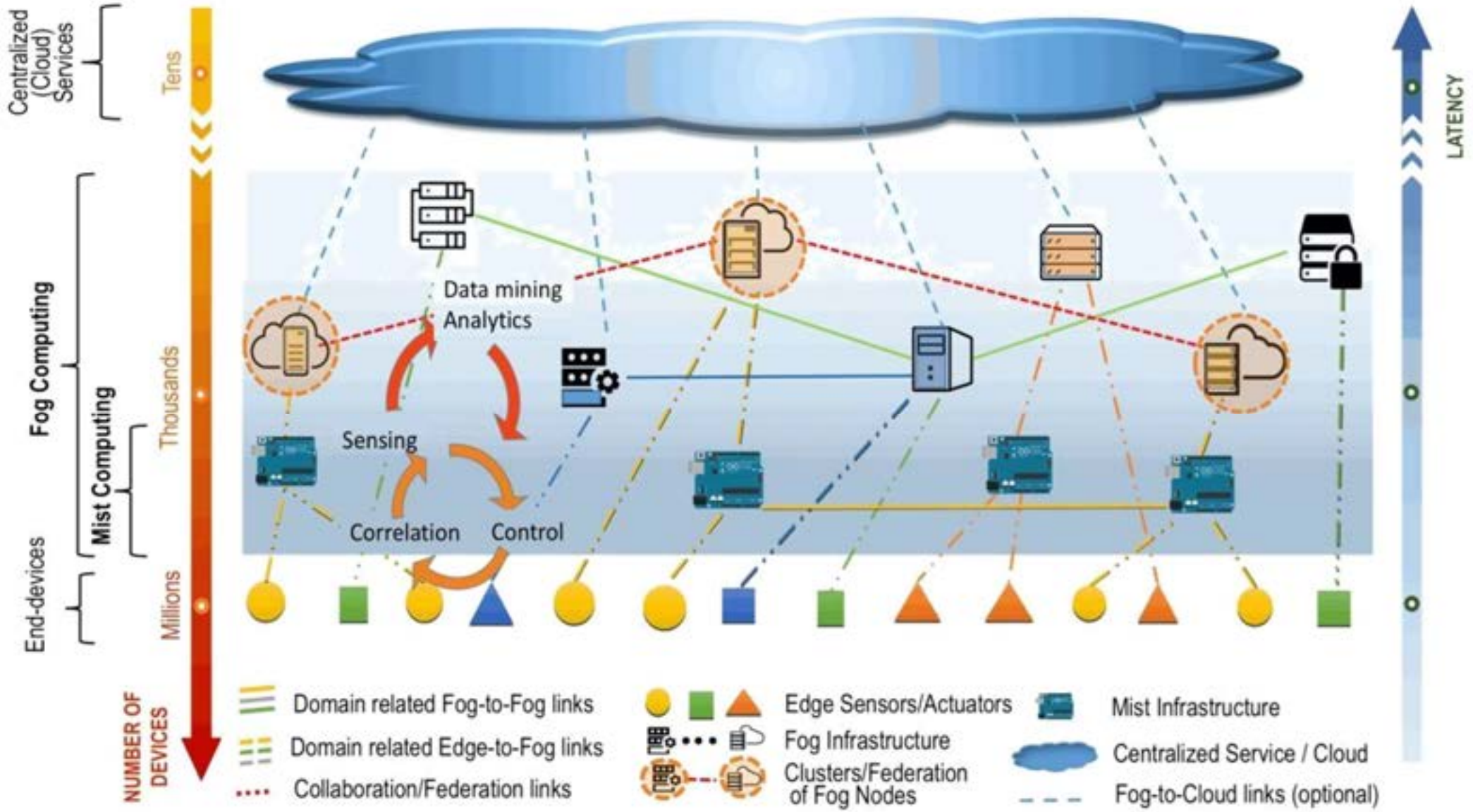
Security Issues

- Biggest security risks associated with DER gateway systems is that they are a single point of failure.
- Attacker could use the gateway
  - to inject malicious code into the DER system.
  - to disrupt the communication between the DER system and the grid.
- Vulnerable to a number of common cyberattacks, such as malware attacks, denial-of-service attacks, and phishing attacks.

- **Auth & Auth Weaknesses**: DER gateways must authenticate and authorize users/devices. Failure here can lead to unauthorized access.
- **Encryption Weaknesses**: Proper encryption is vital to protect data in transit/at rest. Inadequate implementation risks data theft.
- **Software Weaknesses**: Software-based DER gateways need regular patching. Neglect can lead to exploits and gateway control.
- **Physical Security**: Often remote, physical security lapses can grant attackers access, compromising the gateway.

Cloud-based Gateway

- Cloud-based: **Entire controller function in the cloud.**
- Edge and fog integration: **Edge processes data at the source, fog distributes across edge, fog, and cloud based on criticality.**
- Edge computing: **Decentralized data processing at the edge, minimizes network traffic, enables near real-time analysis.**
- Fog computing: **Supports latency-sensitive apps with scalable, multi-tiered systems.**
- Complex deployment: **Integrating edge, fog, and cloud adds complexity, requires careful consideration of data processing locations.**


Centralized (Cloud) Services
Fog Computing
Mist Computing
End-devices
Tens
Thousands
Millions
NUMBER OF DEVICES
LATENCY
Data mining
Analytics
Sensing
Correlation
Control
Domain related Fog-to-Fog links
Domain related Edge-to-Fog links
Collaboration/Federation links
Edge Sensors/Actuators
Fog Infrastructure
Clusters/Federation of Fog Nodes
Mist Infrastructure
Centralized Service / Cloud
Fog-to-Cloud links (optional)

Cloud-based Gateway

Advantages

- **Scalability:** Easily scale to accommodate large-scale deployments.
- **Cost-efficiency:** Lower upfront costs, pay for cloud resources used.
- **Flexibility:** Adapt to changing requirements and updates seamlessly.
- **Easy deployment:** Faster than deploying physical hardware.
- **High availability:** Built-in failover mechanisms and data replication.
- **Advanced analytics:** Take advantage of cloud-based analytics and machine learning.
- **Advanced security:** Advanced analytics and up-to-date threat intelligence can prevent future threats.

Disadvantages

- Latency: May introduce latency for real-time applications.
- Data privacy concerns: Storing sensitive data in the cloud may raise privacy and compliance issues.
- Data transmission costs: Sending large volumes of data to the cloud can be costly.
- Connectivity dependency: Relies on Internet connectivity, which can be a problem in remote environments.
- Security risks: Data transmitted to the cloud may be at risk of security breaches.
- Vendor lock-in: Organizations may become dependent on a specific cloud provider.
- Regulatory compliance: Meeting regulatory compliance requirements can be complex.

Security Advantages

- **Strong security from cloud providers:** Cloud providers invest in security infrastructure and tools to protect against cyber threats.
- **Automatic security updates:** Cloud providers automatically update their infrastructure and software, reducing security risks.
- **High availability and redundancy:** Cloud platforms have multiple data centers and redundancy features to ensure continuous service.
- **Advanced security monitoring and analytics:** Cloud providers offer tools to detect and respond to security threats in real time.
- **Secure user and device access:** Cloud platforms provide tools to control and manage user and device access.
- **Data encryption:** Data transmitted to and from the cloud-based IoT gateway is encrypted using strong encryption protocols.

Security Issues

- **Data privacy:** Storing sensitive data in the cloud can raise privacy and compliance risks.
- **Latency:** Data transmission to and from the cloud can introduce latency, which can be a problem for real-time apps.
- **Data transmission security:** Securing data transmission is crucial. Vulnerabilities can be exploited by attackers.
- **Vendor lock-in:** Organizations may become dependent on a specific cloud provider.
- **Access control:** Strong access control and authentication are essential to prevent unauthorized access.
- **Compliance:** Organizations must comply with industry standards and regulations when deploying cloud-based IoT solutions.
- **DDoS attacks:** Cloud services are susceptible to DDoS attacks. Mitigation strategies and controls are essential.

Fragmented Landscape

Hybrid Gateway

Hybrid gateways combine on-premises and cloud-based benefits, processing sensitive data locally and non-sensitive data in the cloud.

The choice between on-premises, cloud-based, or hybrid IoT gateways depends on specific needs. On-premises prioritizes security and compliance, cloud-based focuses on cost and ease, while hybrid offers a balance.

According to a recent PTC survey, 45% of organizations use on-premises IoT gateways, 35% opt for cloud-based, and 20% favor hybrid gateways, indicating a preference for on-premises with growing interest in cloud-based solutions.

The adoption of hybrid gateways is expected to increase as organizations seek a balanced approach, aiming to combine the strengths of both on-premises and cloud-based solutions.

Hybrid Gateway

- **Integration:** Combines on-prem and cloud processing for flexibility.
- **Latency:** Reduces latency for real-time apps, sends non-time-sensitive data to cloud.
- **Privacy:** Keeps sensitive data on-prem for privacy and compliance.
- **Scalability:** Handles growing number of devices, cost-effective.
- **Complexity:** Implementing and managing can be complex, requires expertise.

Hybrid Gateway

Advantages

- **Low latency:** Processes data locally for real-time response.
- **Privacy:** Sensitive data processed on-prem for compliance and control.
- **Scalability:** Handles growing number of devices, cost-effective.
- **High availability:** Local processing ensures continued functionality.
- **Security:** Data transmitted within organization's network, reducing threats.

Disadvantages

- Complexity: Requires expertise, more complex than on-prem or cloud-based solutions.
- Initial setup: Learning curve, may require additional integration.
- Maintenance overhead: Increased maintenance workload for both on-prem and cloud components.
- Hybrid integration challenges: Seamless integration can be challenging, requires careful design and monitoring.
- Resource management: Complex to manage resources between on-prem and cloud environments.
- Data routing: Complex decision-making process to determine data direction.

Security Advantages

- **Enhanced Security:** Hybrid gateways offer robust security by processing sensitive data on-premise and less sensitive data in the cloud, reducing the attack surface.
- **Improved Data Protection:** They enhance data protection through a mix of on-premises and cloud-based security measures, including encryption and restricted access.
- **Advanced Visibility and Control:** Hybrid gateways boost visibility and control over IoT data and traffic, enabling quicker threat detection and response.
- **Streamlined Compliance:** They aid in compliance with data privacy and security regulations by enabling on-premise storage and processing of sensitive data.

Security Issues

- **Complexity:** Hybrid gateways are more complex to configure and manage than standalone options, posing challenges for effective security implementation.
- **Security Vulnerabilities**: They may face security vulnerabilities in both on-premise and cloud components, increasing the risk to the gateway and processed data.
- **Security Gaps:** Poor integration between on-premise and cloud components can create exploitable security gaps.
- **Data Leakage:** Inadequate data protection at both levels can lead to potential data leakage risks.

Why Hybrid Approach?

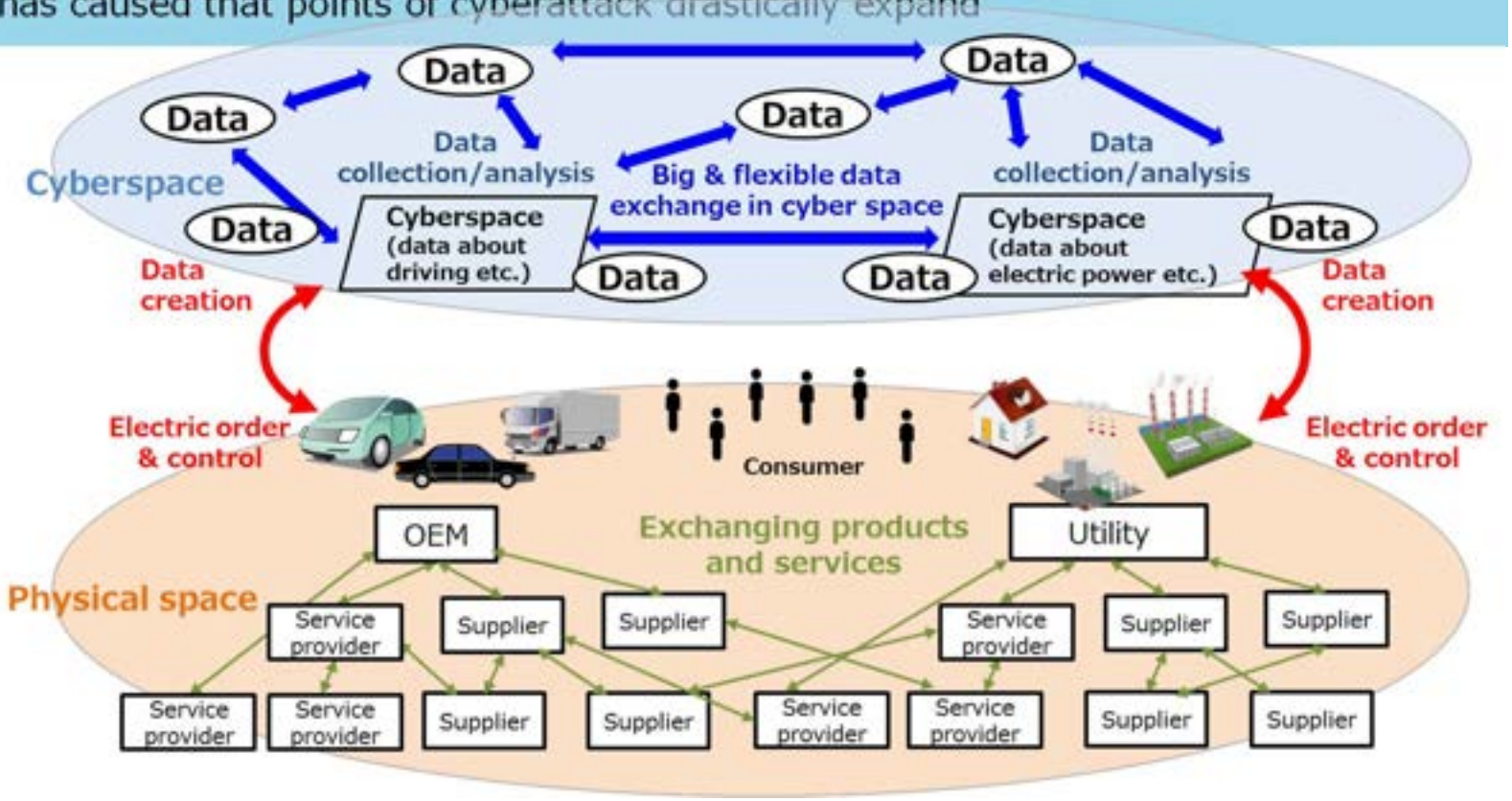
- Performance: Processes data locally for real-time response, critical for low-latency applications.
- Privacy: Sensitive data kept on-premise for control and compliance.
- Scalability: Leverages cloud resources for non-time-sensitive tasks, cost-effective.
- Resilience: Local processing ensures high availability, even with internet outages.
- Security: Minimal attack surface by processing sensitive data on-premise.
- Customization: Organizations can tailor the model to their needs.
- Compliance: Meets data sovereignty laws by keeping data within geographical boundaries.
- Traffic optimization: Reduces network congestion by sending only relevant data to the cloud.

Moving Forward..

- **Leverage Hybrid Controllers**: Use a hybrid controller approach to combine on-premises and cloud-based controllers for benefits like IoT communication using physical controllers and cloud-based virtual controllers.
- **Address Security Risks**: Mitigate security risks associated with hybrid controllers through strong encryption and access control measures.
- **Consider Specific Needs**: When designing your hybrid controller architecture, consider data types, latency requirements, and budget to tailor it to your needs.
- **Choose Reputable Vendors**: Select a secure, scalable, and manageable hybrid controller solution from a reputable vendor.
- **Simplify Integration**: Opt for a single cloud platform for your hybrid controller to simplify integration and management.
- **Utilize Managed Service Providers**: Consider using managed service providers (MSPs) for implementing and managing your hybrid controller solution, especially if you lack in-house expertise.
- **Regularly Review Architecture**: Periodically review your hybrid controller architecture to ensure it meets evolving needs, keeping up with technology trends and best practices.

Cyber Physical System

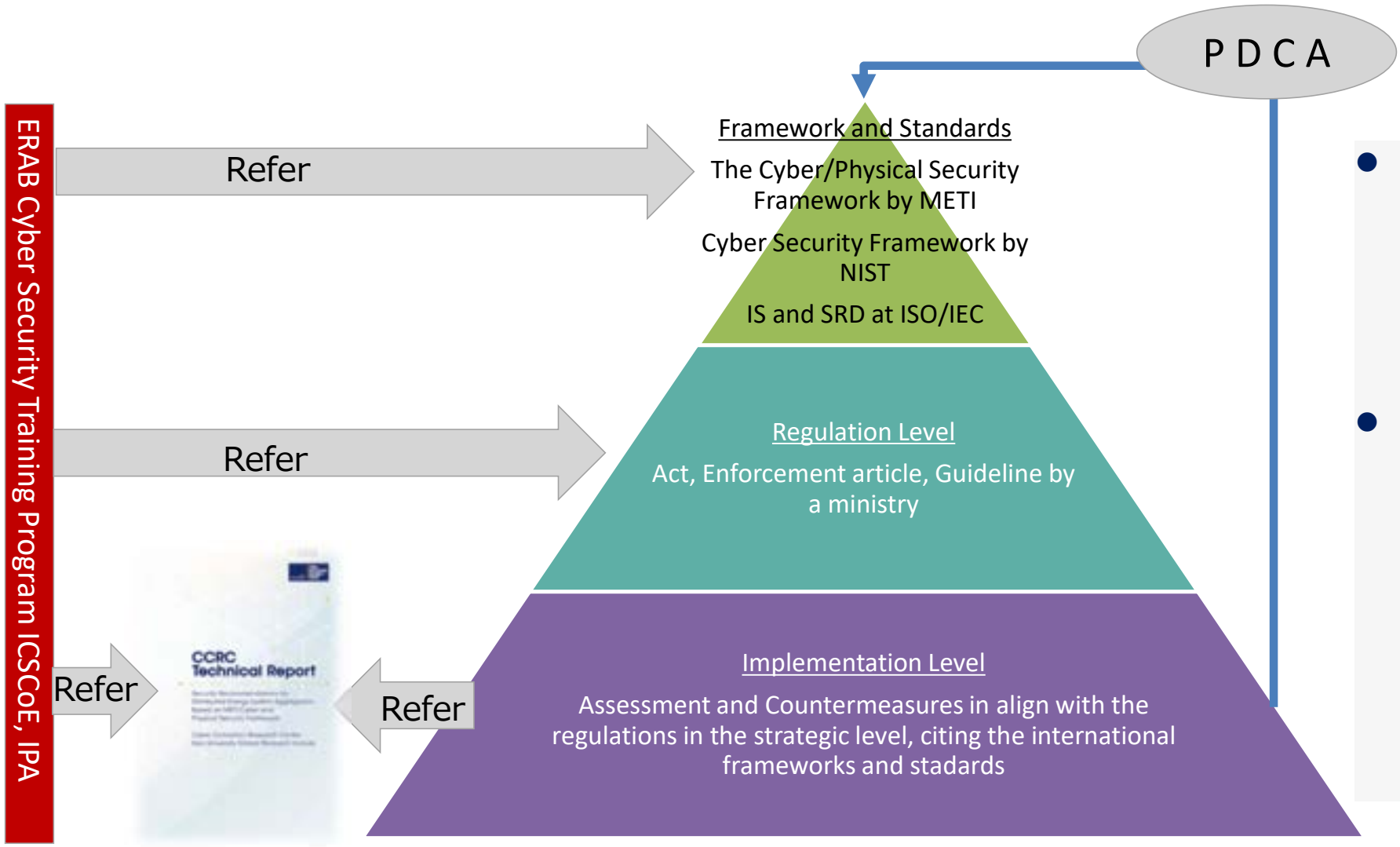
- Cyberspace and Physical space will be highly integrated
  - Two spaces interacting with each other increase the impact of the damages on physical space.
  - It has caused that points of cyberattack drastically expand



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Security implementation example
ERAB case in Japan
Y2023

The security triangle of Energy Resource Aggregation Business



- Japanese aggregators develop security countermeasures ,referring CCRC Technical Report.
- In Japan, a good coordinated triangle exists from implementation to the high-level framework.

The Cyber/Physical Security Framework [CPSF] by METI, Japanese Government

- In “Society 5.0” which is realized by IoT and AI, supply chain is transforming from traditional linear style to non-linear style where various kinds of connections exist. The Cyber/Physical Security Framework grasps the industrial society where value is created as Three Layers composed of Six Elements.

The Third Layer
(Data circulation)

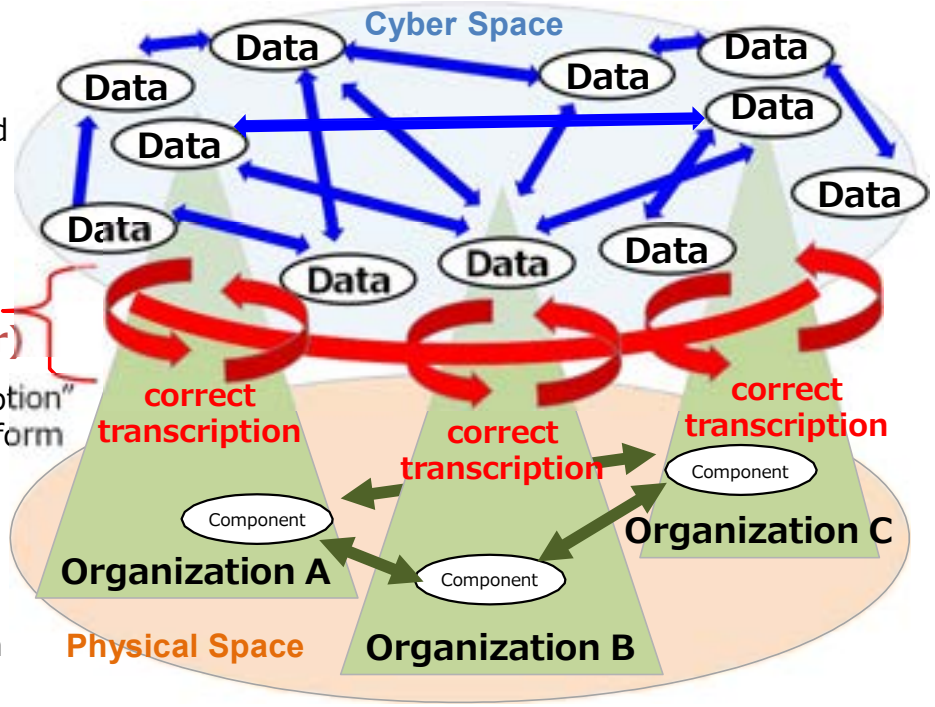
- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer
(Cyber to physical/Physical to cyber)

- Trustworthiness of function for “correct transcription” from cyber to physical / from physical to cyber form

The First Layer
(Relationship among Organizations)

- Trustworthiness of each organization based on appropriate management



◆**Six Elements:** **Organization, people, component, data, procedure, system**

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Six elements in CPSF

- It is necessary to grasp fixed business assets. In the CPSF, the elements are shown by 6 elements: the organization, the people, the components, the data, the procedure, and the system

Element	Definition
Organization	Companies, groups, and organizations that comprise the value creation processes
People	People belonging to organizations, and people directly participating in the value creation process
Components	Hardware, software, and parts, including operating devices
Data	Information collected in physical space, and information edited through sharing, analyzing, and simulating it
Procedure	Sequences of activities to achieve the defined purpose
System	Mechanisms or infrastructures configured with components for the defined purpose

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Compatibility between CPSF in JP and CSF in U.S

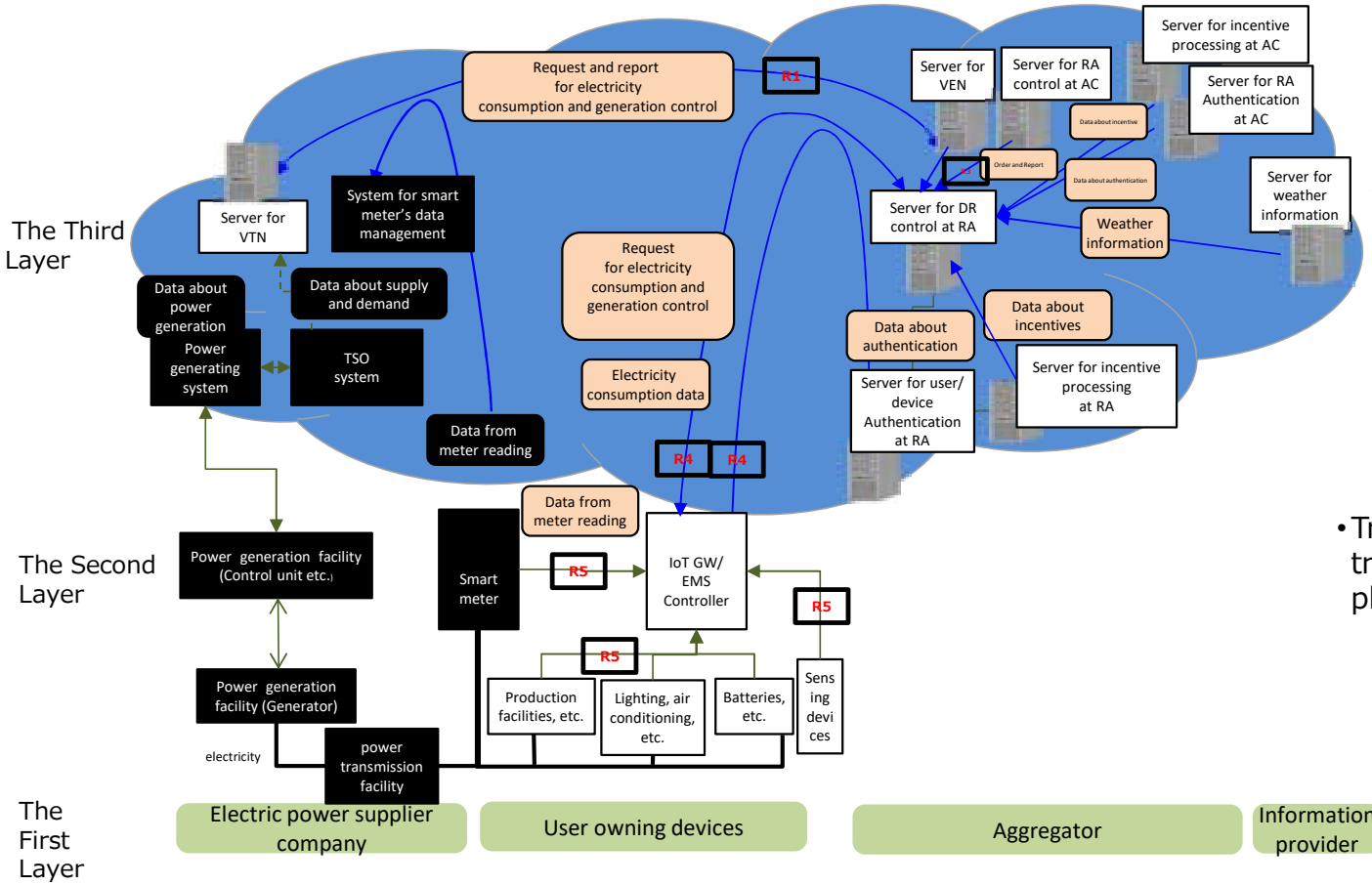
- Cyber/Physical Security Framework in J.P
  - The Cyber/Physical Security Framework (meti.go.jp)
- Cybersecurity Framework Version 1.1 in U.S.
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Category names in CPSF	Acronym	Related category names in CSF
Asset Management	CPSF.AM	ID.AM (Asset Management)
Business Environment	CPSF.BE	ID.BE (Business Environment)
Governance	CPSF.GV	ID.GV (Governance)
Risk Assessment	CPSF.RA	ID.RA (Risk Assessment)
Risk Management Strategy	CPSF.RM	ID.RM (Risk Management Strategy)
Supply Chain Risk Management	CPSF.SC	ID.SC (Supply Chain Risk Management)
Identity Management, Authentication, and Access Control	CPSF.AC	PR.AC (Identity Management and Access Control)
Awareness and Training	CPSF.AT	PR.AT (Awareness and Training)
Data Security	CPSF.DS	PR.DS (Data Security)
Information Protection Processes and Procedures	CPSF.IP	PR.IP (Information Protection Processes and Procedures)
Maintenance	CPSF.MA	PR.MA (Maintenance)
Protective Technology	CPSF.PT	PR.PT (Protective Technology)
Anomalies and Events	CPSF.AE	DE.AE (Anomalies and Events)
Security Continuous Monitoring	CPSF.CM	DE.CM (Security Continuous Monitoring)
Detection Processes	CPSF.DP	DE.DP (Detection Processes)
Response Planning	CPSF.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
Communications	CPSF.CO	RS.CO (Communications) RC.CO (Communications)
Analysis	CPSF.AN	RS.AN (Analysis)
Mitigation	CPSF.MI	RS.MI (Mitigation)
Improvements	CPSF.IM	RS.IM (Improvements) RC.IM (Improvements)

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Mapping Energy Resource Aggregation Business [ERAB] System on CPSF

◆**Six Elements:** **Organization, people, component, data, procedure, system**



The Third Layer (Data circulation)

- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

The First Layer (Relationship among Organizations)

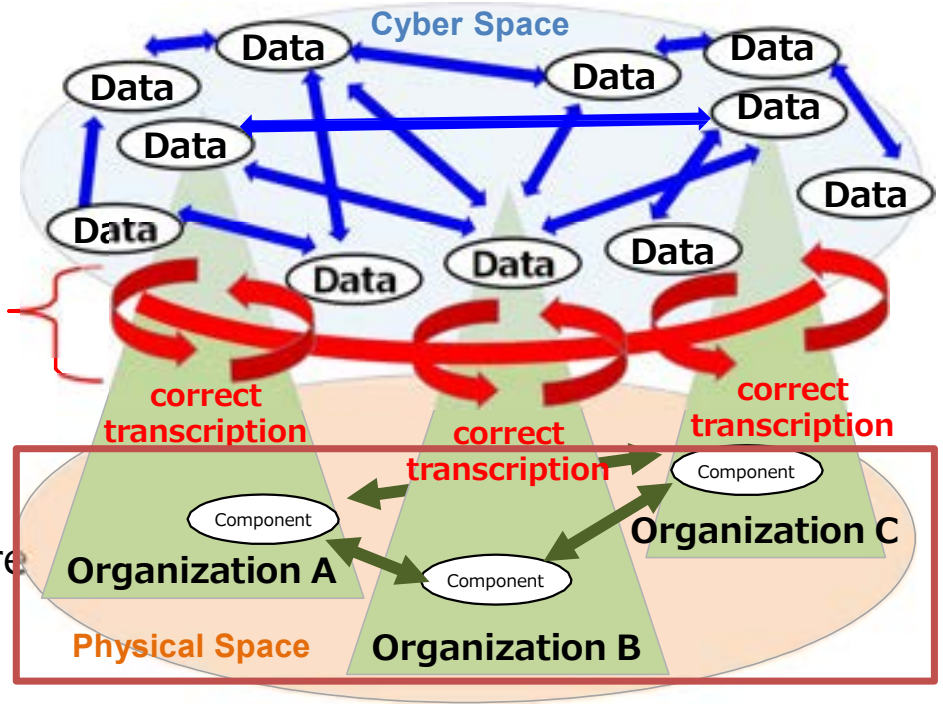
- Trustworthiness of each organization based on appropriate management

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

First Layer in CPSF

- The First Layer (Relationship among Organizations)
  - The first layer aims to ensure trust in the management of an organization. It has been adopted to achieve security across supply chains.

- Certification programs such as ISMS (based on ISO/IEC 27001) focus on confirming trust in company management
- The first layer in CPSF aims to achieve shared and certified security policies as a basis for promoting trust.
- In Cyber-Physical system, where cyber and physical space are integrated, it is impossible to ensure trust throughout the entire value creation process only by security implementation in the first layer.

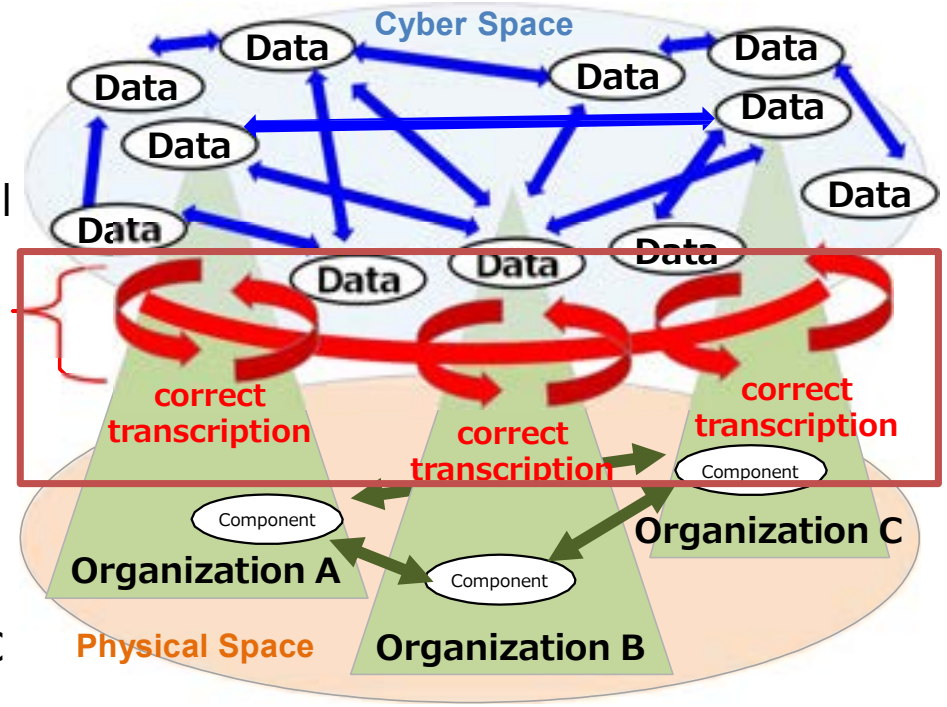


Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Second Layer in CPSF

- The Second Layer (connections between cyberspace and physical space)
  - Unreliable interactions between cyberspace and physical space could cause uncertainty throughout industrial society.

- The second layer is based on the accuracy and trustworthiness of data transcription and transfer (including accurate translation) between cyberspace and physical space.
- Certification programs such as ISO/IEC 27036 focus on confirming trustworthiness in transcription
- It is impossible to ensure trust throughout the entire value creation process only by ISO/IEC 27036.



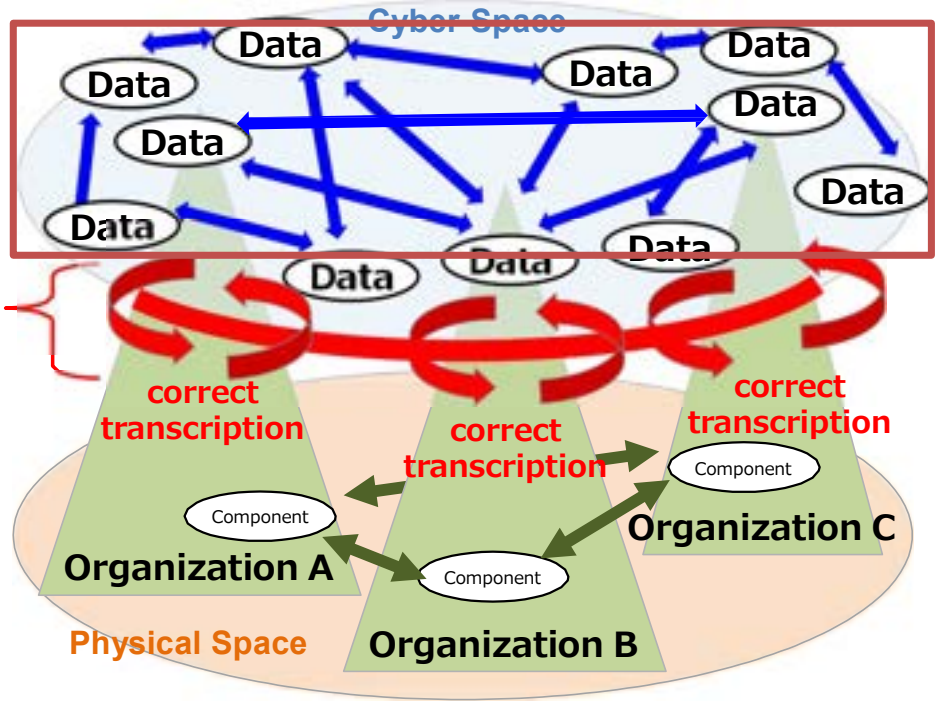
Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Third Layer in CPSF

- The Third Layer (connections in cyberspace)
  - security measures need to be implemented in the third layer for data distribution and storage and appropriate editing and processing

•Certification programs such as ISO/IEC 27017 focus on confirming trustworthiness in cloud data storage

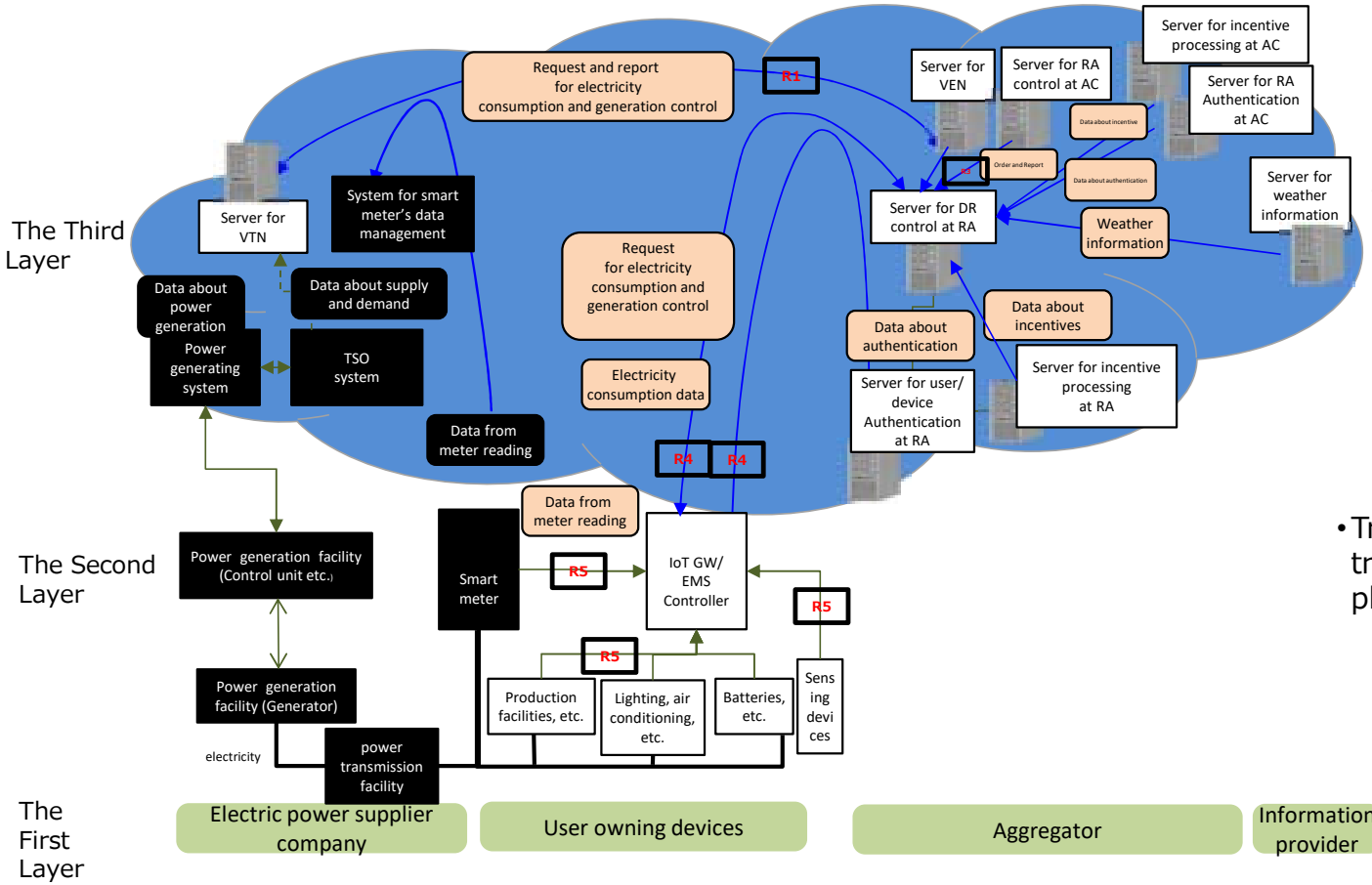
•It is impossible to ensure trust throughout the entire value creation process only by ISO/IEC 27017.



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Mapping Energy Resource Aggregation Business [ERAB] System on CPSF

◆**Six Elements:** **Organization, people, component, data, procedure, system**



The Third Layer (Data circulation)

- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

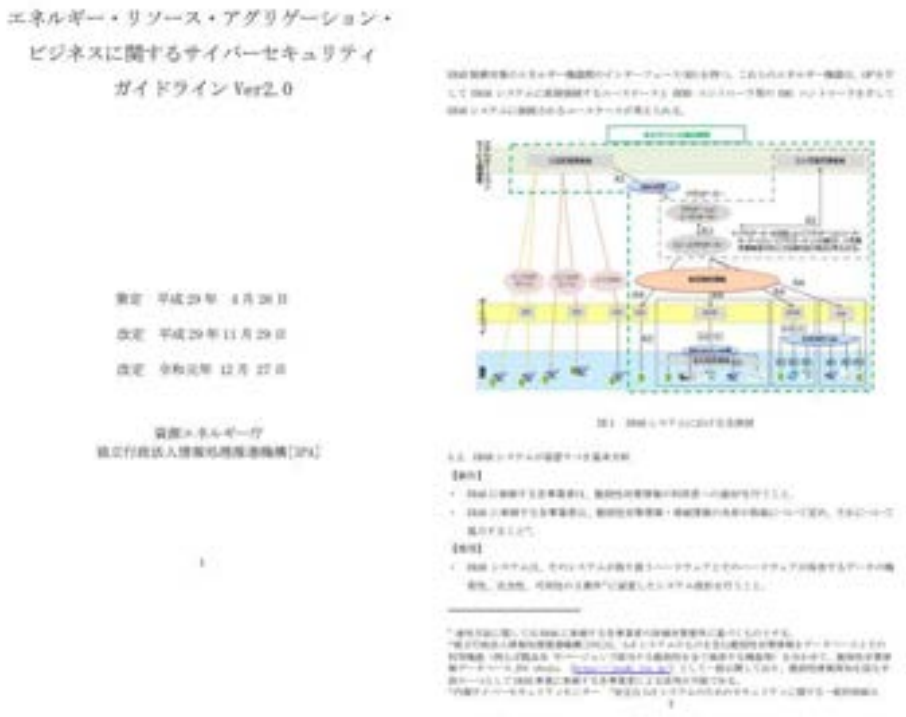
The First Layer (Relationship among Organizations)

- Trustworthiness of each organization based on appropriate management

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Cybersecurity Guideline for Energy Resource Aggregation Business ver.2.0

- Agency for Natural Resources and Energy and Information-technology Promotion Agency [IPA] provide the guideline showing the cybersecurity measures that businesses participants in ERAB should take.


エネルギー・リソース・アグリゲーション・
ビジネスに関するサイバーセキュリティ
ガイドライン Ver2.0

- Japanese original version is available at:
  - https://www.meti.go.jp/english/press/2019/1227_005.html
- English translation with a research purpose is available at:
  - https://www.enecho.meti.go.jp/en/category/vpp_dr/data/cybersecurity_guidelines_for_erab.pdf

Japan case: Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0

- Article 3.6 defines the design on cybersecurity measures for ERAB system

Process	Content
Step1	Clarify the overall system configuration and responsibility demarcation point of intended IoT product or service.
Step2	Clarify the information, function and assets for protection in the system
Strep3	Clarify the possible threat for the information, function and assets for protection
Step4	Clarify countermeasures (best practice) against threat
Step5	Select measures to implement considering threat level, damage level, cost, etc.
Step6	Verify the implementation of countermeasures that the mandatory items are prioritized through third-party audits (including certification), educational programs.
Step7	Design, operate and train the way to respond to accidents

Source: Agency for Natural Resources and Energy Information-technology Promotion Agency(2019) Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0

CCRC CONTRIBUTES TO DESIGN ERAB SYSTEM SECURITY

TOKYO, JAPAN
KEIO UNIVERSITY
CYBER CIVILIZATION RESEARCH CENTER

- **In 2021, CCRC published the technical report on "Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework", showing 51 recommendations to be countermeasures to the major vulnerabilities of ERAB system.**
  - The report is backed by 5 years experience of running a prototype system
  - The full report is available at
    - https://www.ccrc.keio.ac.jp/ccrc-technical-report-202109/

ERAB Cyber Security Training Program ICSCoE, IPA

- Industrial Cyber Security Center of Excellence in IPA (ICSCoE) has provided a training program to help aggregators have an appropriate security design about an electricity aggregation system.
- The program has complied with “Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0” published in Agency for Natural Resources and Energy in Japanese Government and IPA, referring “The Cyber/Physical Security Framework” in METI and CCRC Technical Report “Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework” published in Keio University

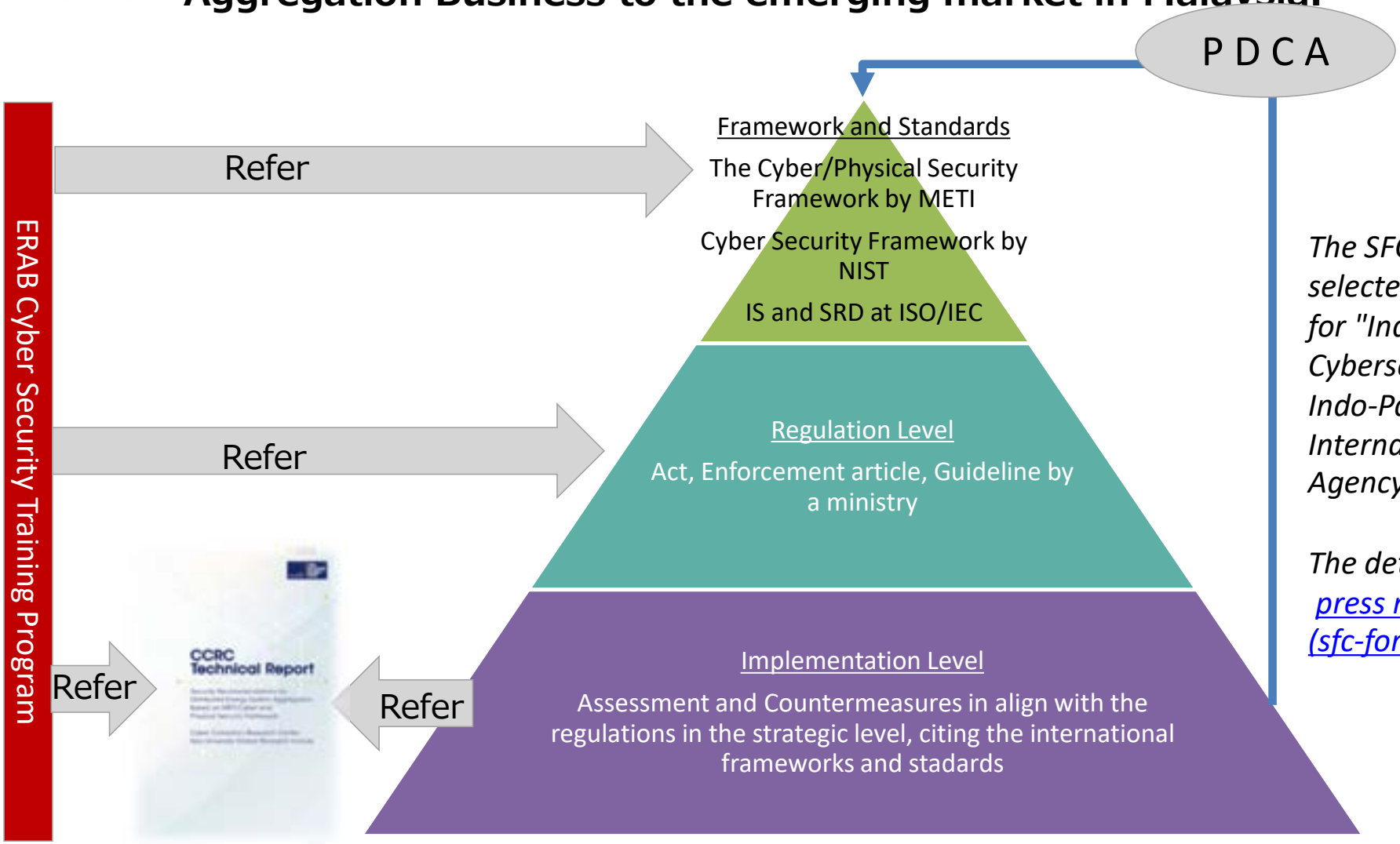
The training program has the three components:

- Learn the related regulations and bibliographies
- Exercise a risk assessment
- Experience multiple hazards on a demo system

Common Criteria: ISO/IEC 15408 is the standard to ensure IT product security at a customer premise

- ISO/IEC 15408 as it were Common Criteria (CC) is the standard dealing with product safety.
  - The basis for evaluation of security properties of IT products.
  - Globally recognized certification.
  - **Malaysia and Japan have partnered as the Certificate Authorizing Member**

As per CPSF, Japanese and Malaysian security experts have launched empirical study applying the security triangle of Energy Resource Aggregation Business to the emerging market in Malaysia.



The SFC Forum has been selected to conduct the survey for "Industrial Control Systems Cybersecurity Training for Indo-Pacific Region" for Japan International Cooperation Agency （JICA）

The details is at:
press release_en_20230900 (sfc-forum.or.jp)