ERIA-DP-2025-5

ERIA Discussion Paper Series
No. 551

Security by Design for Cyber and Physical Systems for Driving Energy Transformation through Decarbonisation, Decentralisation, and Digitalisation: CPSF and ERAB Initiatives in 2024

Masaki UMEJIMA[*]
Convener of Development Plan, IEC System Committee Smart Energy

Jun MURAI
Senior Advanced Research Project Professor, Cyber and Civilization Research Centre, Keio University (CCRC), Japan

Naoto OKURA
Director General for Research and Policy Design, ERIA

July 2025

Abstract: *Rapid economic growth in Southeast Asia has significantly increased energy demand amidst a rapidly evolving global energy landscape, characterised by a growing reliance on distributed energy resources (DERs) and distributed energy systems (DESs). The Energy Resource Aggregation Business (ERAB) has emerged as a vital approach for managing and optimising these resources through open-standard interfaces and Internet-based architectures, underpinned by open, autonomous, distributed, and globally governed systems.*

However, most organisations today face considerable challenges due to the rapid proliferation of potentially vulnerable DERs and DESs. Consequently, ERAB systems – comprising DERs and DESs – must be designed to securely isolate network components while minimising impacts on the broader network, consumers, and business partners in the event of a breach.

The authors, convened under the ERIA study group, conclude that in addition to the critical role of standardising hardware and software security protocols, the three-layer, six-element model of the Japanese Ministry of Economy, Trade and Industry's Cyber/Physical Security Framework (CPSF) is highly applicable to ERAB security design. This model supports the configuration of DERs according to international standards within the global supply chain.

Keywords: Technological Change, Open Innovation

JEL classification: O360

[*] The authors thank co-authors: Dr Keiko Okawa (Advanced Research Project Professor, Keio University, Japan), Dr Sureswaran Ramadass (Chairman of APAC IPv6 Council), Dr Selvakumar Manickam (Head of Cyber Security Research Centre, University Sains Malaysia, Malaysia), Dr Ary Setijadi Prihatmanto(Head of the Centre for Excellence in Defence and Security Science and Technology, Bandung Institute of Technology, Indonesia), Mr Basuki Suhardiman(Bandung Institute of Technology, Indonesia), Assoc. Prof. Krerk Piromsopa (Cybersecurity Research Team, Department of Computer Engineering, Chulalongkorn University, Thailand), Dr Dechanuchit Katanyutaveetip (Dean, Faculty of Information Technology, Siam University, Thailand), Dr Waraporn Promwikorn (Assistant Secretary-General, National Cyber Security Committee, Thailand), Air Vice Marshal Chalermchai Wonggate (Director of Cybersecurity Research Centre, National Cyber Security Agency, Thailand), Dr Soontorn Sirapaisan (Acting Head of the Research and Research Collaboration Section, National Cyber Security Agency, Thailand), Dr Kalika Sooksomboon (Senior Researcher, National Electronics and Computer Technology Cenre, Thailand), Mr Akinori Kahata (Deputy Director, Agency for Natural Resources and Energy in Ministry of Economy, Trade and Industry, Japan), and Mr Kei Sudo (Former Programme Manager on Energy, ERIA).

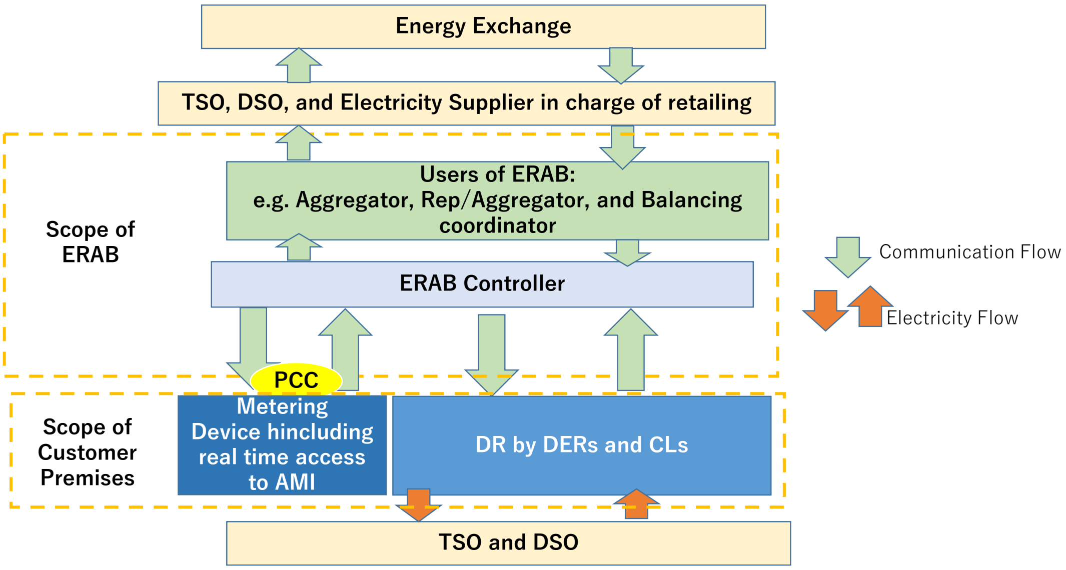
1. ERAB as A New Scenario in The Energy System

1.1. IEC SRD63443 as the new international standard for ERAB is in progress

The global energy landscape is rapidly evolving with an increasing reliance on distributed energy resources (DERs) and smart grids. The Energy Resource Aggregation Business (ERAB) has emerged as crucial for managing and optimising these resources with an open standard interface.

As ERAB plays a vital role in energy systems, International Electrotechnical Commission (IEC) is developing a new international standard called the Systems Reference Deliverable (SRD 63443) based on ERAB implementation in Japan. This new standard aims to define ERAB as a system to restrain or elevate the power generation of distributed energy resources (DERs) and the power demands of controllable loads (CLs) at customer premises, in accordance with performance measurements from the metering device at the point of common coupling (PCC). It enables real-time data access from customer premises and responds to requests from the transmission service operator (TSO), distribution system operator (DSO), electricity supplier, and energy exchange, as illustrated in Figure 1.

Figure 1: Position of ERAB in the Electricity System


Energy Exchange
TSO, DSO, and Electricity Supplier in charge of retailing
Scope of ERAB
Users of ERAB:
e.g. Aggregator, Rep/Aggregator, and Balancing coordinator
ERAB Controller
Communication Flow
Electricity Flow
PCC
Scope of Customer Premises
Metering Device hincluding real time access to AMI
DR by DERs and CLs
TSO and DSO

AMI = advanced metering infrastructure, CL = controllable load, DER = distributed energy resource, DR = demand response, DSO = distributed system operation, PCC = point of common coupling, TSO = transmission service operator.
Source: Authors.

An aggregator contracts with several other network users to combine the effects of smaller loads or DERs for actions, such as demand response or ancillary services. This model provides information regarding end-user-based adjustments in the control timing and electricity consumption.

The flexibility of the electricity infrastructure is managed through dynamic pricing policies for kilowatt-hours (kWh) and kilowatts (kW) based on scheduling algorithms. Rising demand, power shortages, power quality issues, rolling blackouts, and electricity price spikes have led many utility customers to seek alternative, high-quality, and reliable electricity sources.

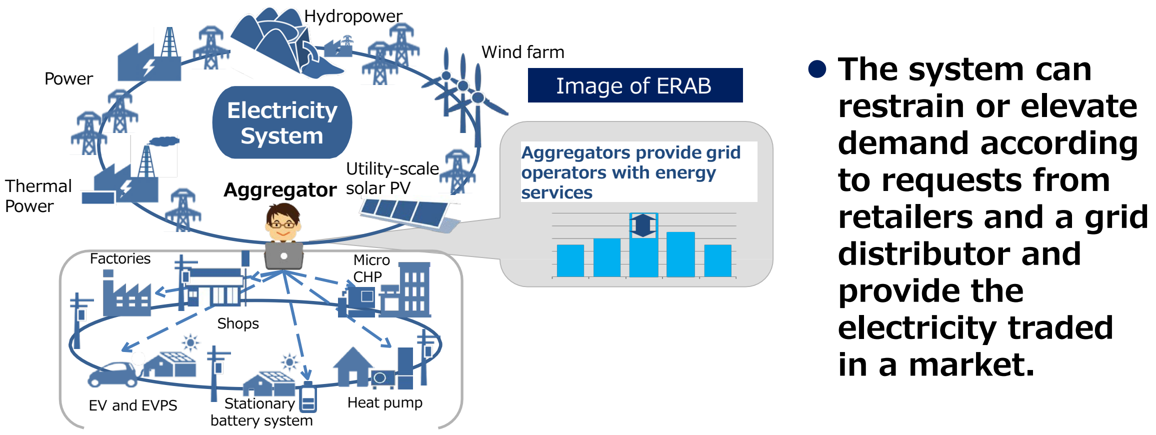
A DER, which is a small-scale power generation source located near where electricity is consumed (e.g. homes or businesses), can provide an alternative to the traditional electric power grid.

In conventional power systems, the balance between supply and demand is adjusted by the TSO and DSO controlling the power generation facilities on the supplier side, enforcing the same amounts of demand and supply simultaneously on the TSO and DSO. However, the widespread use of DERs and CLs with network access has enabled them to be configured as virtual systems on the demand side. In addition, real-time data access to a metering device allows measurement of the performance of aggregating these devices using trustworthiness data. Similar to drastic changes in the electricity system, ERAB provides a new service scenario that contributes to the balance of supply and demand within the electricity system.

ERAB provides two types of services: demand restraint and demand increase. The former model removes tight supply and demand by effectively shaving or shifting the peak demand. The latter model contributes to the effective use of energy by shifting demand in response to the excessive power supply owing to the expansion of the introduction of renewable energy, as well as the improvement of energy autonomy by aggregating DERs and CLs with a power storage function.

However, the electric utility service mandates that supply and demand remain balanced for the grid to function correctly. Based on this principle, balancing electricity is traded in a marketplace known as the balancing market. Aggregators aim to provide the capacity necessary to achieve balance whilst reducing dependency on large-scale power plants. This is achieved by controlling the DERs by implementing an energy management system at the customer premises. Aggregators reserve balancing capacity and agree to hold it in response to the requests of TSOs. The arrangement lasts for the duration of the contract, for which generators or other demand-side participants submit bids to deliver balancing energy in real time. Figure 2 shows the ERAB service image.

Figure 2: Image of the ERAB Service

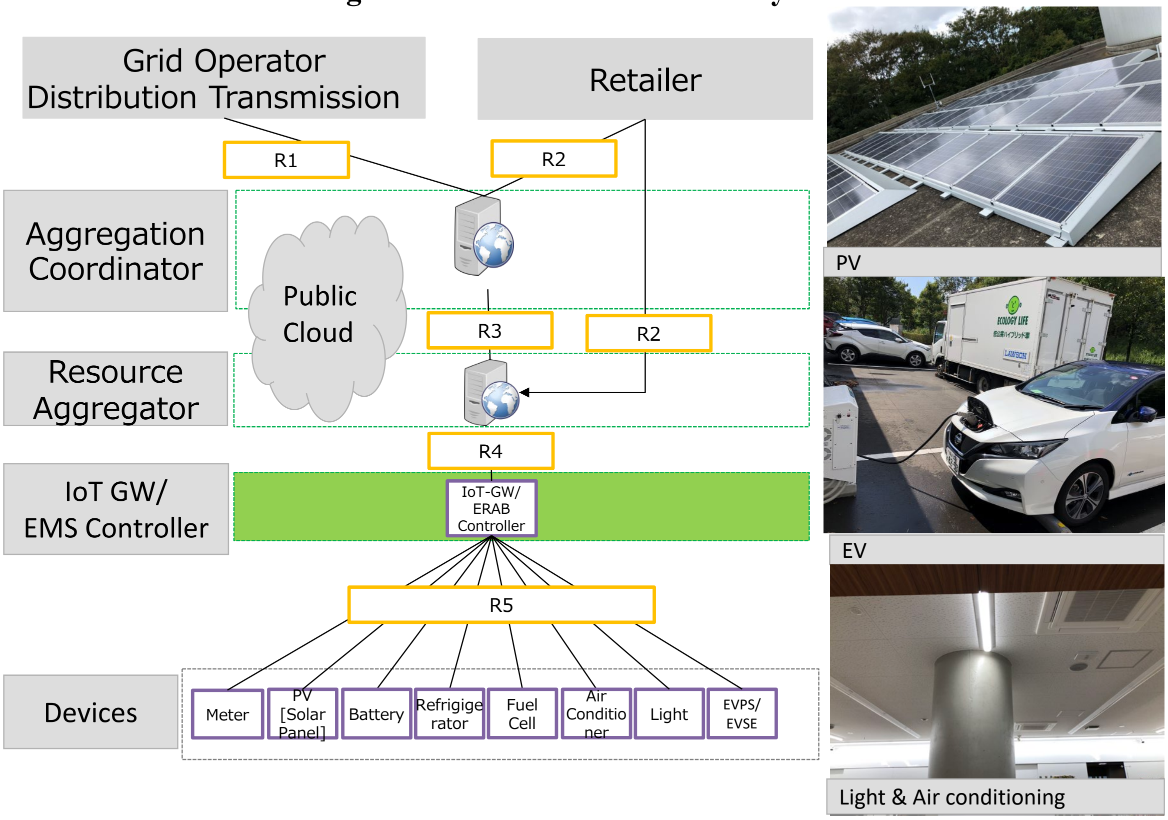


- **The system can restrain or elevate demand according to requests from retailers and a grid distributor and provide the electricity traded in a market.**

EV = electric vehicle, EVPS = electric vehicle power station, PV = photovoltaic.
Source: Authors.

The ERAB coordinates the requests and reports from/to ERAB participants, such as the TSO, DSO, and electricity supplier, and manages the remote control of the DERs and CLs executed through the ERAB controller, which provides site-specific DER management. ERAB is faster and less expensive than the construction of large central power plants and high-voltage transmission lines, and it offers consumers the potential for lower costs, higher service reliability, enhanced energy quality, efficiency, independence, and potentially greater resilience. The use of renewable and distributed energy generation technologies such as wind, photovoltaic, geothermal, biomass, and hydroelectric power can also provide significant environmental benefits. ERAB combines DERs to function as a self-contained unit that participates in the electricity market or ancillary aggregating services. If ERAB is widely implemented, electricity companies can save the costs of constructing and maintaining spare generation facilities that are only used to meet temporary surges in electrical demand. Additionally, ERAB will facilitate the expansion of renewable energy sources, enabling a stable electricity supply. Figure 3 shows the outlook of the ERAB system.

Figure 3: Outlook of the ERAB System



Source: Authors.

ERAB is a system that can supply power and/or help balance power, and restrain or increase power demand by aggregating DERs, enabling demand response (DR) as a service model. ERAB systems operate with power transmission and distribution companies, energy retailers, electricity producers, users, and prospective partners, including renewable energy power companies.

- The ERAB system is one of the key solutions used to integrate DERs into the grid, thereby reducing fluctuations caused by renewable energy. The ERAB system enables the monitoring of the performance of charging and discharging DERs in 1-minute intervals.
- The monitoring function (measurement) and the timing of the charging/discharging operations are critical points in the ERAB system.
- Management (i.e. monitoring the quality of ERAB operations) is also an important function for understanding how devices are placed in various geographies.

1.2. Application of an Open-standard Language to DERs in ERAB: ISO/IEC14543-4-3

It is recommended that ERAB use open-standard languages to facilitate DERs, such as home appliances (e.g. air conditioners and lighting equipment) that receive and answer DR signals from TSOs. Therefore, for implementation in Japan, two IEC specifications are recommended: ISO/IEC62746-10-1 (Open ADR) for communication between the TSO and a resource aggregator and ISO/IEC14543-4-3(ECHONET Lite) for communication between DERs.

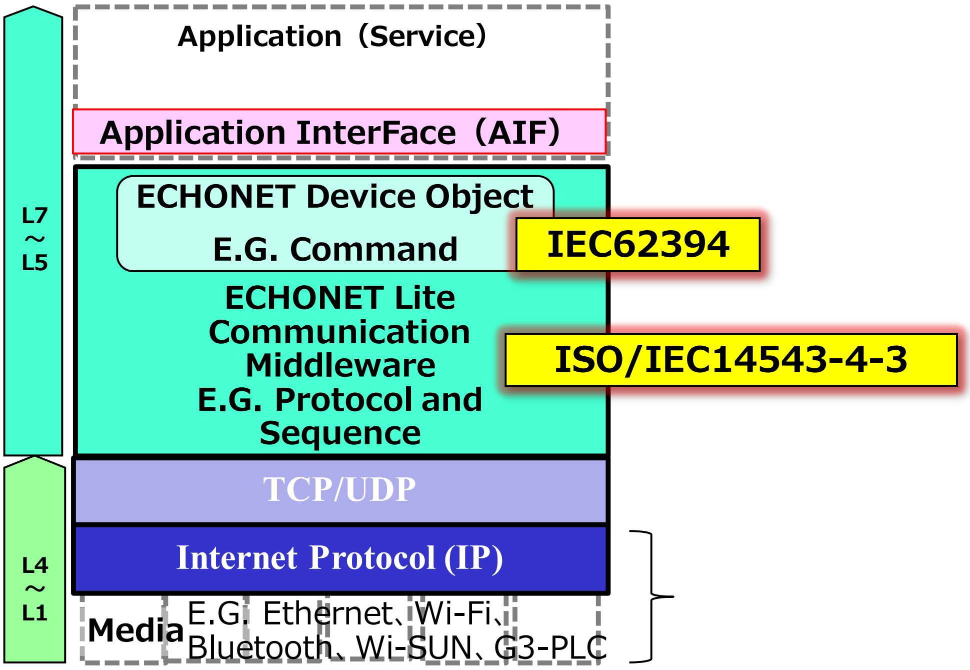
Open ADR is an open protocol that enables two-way information exchange on a smart grid. It standardises the message format used for DR and DER management, so that signals regarding dynamic prices can be exchanged in a uniform and interoperable fashion amongst utilities. The adoption of Open ADR 2.0 has occurred throughout many parts of North America, including California, Nevada, Texas, Florida, Arizona, and Hawaii, and across the globe in Europe, China, Japan, and the Republic of Korea.

When a disastrous earthquake and tsunami in 2011 triggered a nuclear catastrophe in Fukushima, Japan, a public-private partnership played a vital role in adopting a new approach in which every home and store appliance had network access and open-source interfaces. This ambitious project, called the Energy Conservation and Homecare Network (ECHONET) Lite Initiative, began with 22 industrial participants in 2011. ECHONET Lite specialises in handling small amounts of light data to ensure the smooth processing of powerless central processing units (e.g. 8-bit microcomputers) installed in sensors and large household electrical appliances (known as ‘white goods’).

ECHONET Lite is the successor to ECHONET. ECHONET’s weakness was that it did not support the global trend toward the increased use of Internet Protocol (IP) at the network layer, as it adopted a vertical integration strategy by defining all layers from the physical media to the application layers. In particular, the enforcement of the ECHONET address, which is not IP-based, presented a major barrier to the implementation of ECHONET. In response to requests from the public and private sectors to adapt ECHONET to be IP-based, ECHONET Lite was introduced in 2011. The specification of ECHONET Lite defines the application layer and specifies that the network layer utilises IP. In 2020, ECHONET Lite became ISO/IEC14543-4-3. Its management organisation, called ECHONET Consortium, has members from over 250 companies and institutions, including Panasonic, Toshiba, NTT, Softbank, and SMA in Germany, to name a few. The ECHONET Lite specification covers over

100 different home appliances and DERs (e.g. air conditioners, lights, photovoltaic solar cells, fuel cells, storage batteries, and power meters). DERs compatible with ECHONET Lite have increased, such that ECHONET Lite appliances can be purchased in retail stores in Japan and Asia without paying a premium price. In 2018, approximately 150 million DERs, including 82 million nationwide smart meters in Japan, could speak using ECHONET Lite over IP. The protocol design of ECHONET Lite is shown in Figure 4.

Figure 4: Protocol Stack with IEC14543-4-3 (ECHONET Lite) for DERs



Application（Service)
Application InterFace（AIF)
ECHONET Device Object
E.G. Command
IEC62394
ECHONET Lite Communication Middleware
E.G. Protocol and Sequence
ISO/IEC14543-4-3
TCP/UDP
Internet Protocol (IP)
Media
E.G. Ethernet、Wi-Fi、Bluetooth、Wi-SUN、G3-PLC
L7 ～ L5
L4 ～ L1

Source: Authors.

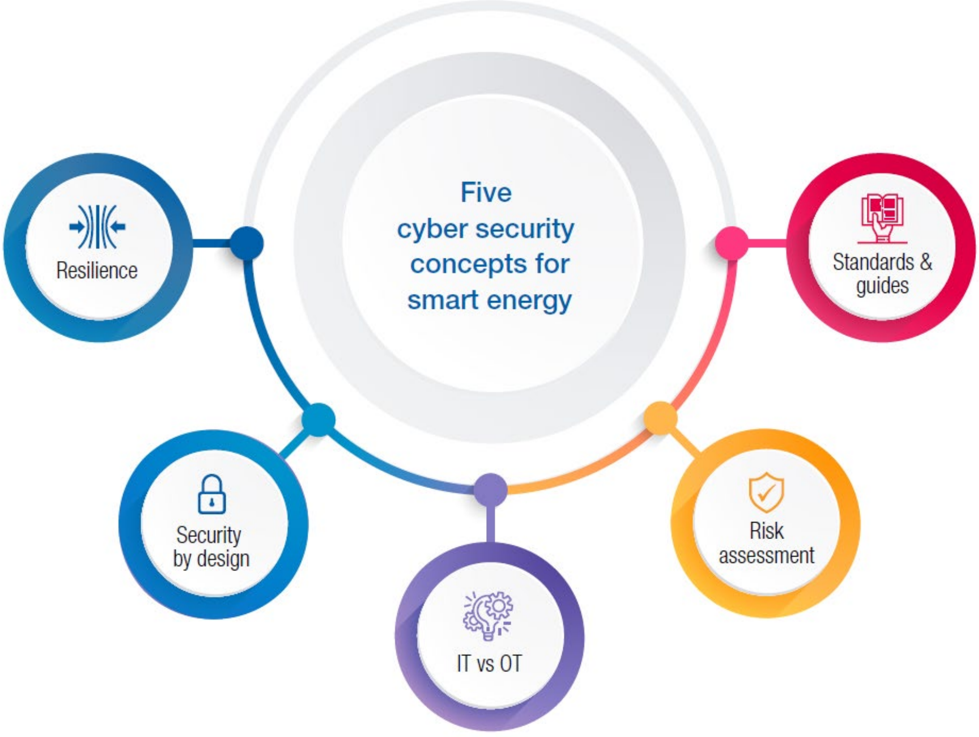
2. Security by Design in ERAB

2.1. Compliance with International Standards

A cyber-physical system (CPS) is defined as a system with digital, analogue, physical, and human components that interact with each other and are engineered to function through integrated physics and logic. A CPS explicitly comprises operational technologies (OT) and information technologies (IT). In a CPS, the supply chain, which is a series of activities undertaken by companies to create added value, will also change its form. The existing supply chain is a rigid, linear structure of strict planning, including design, the procurement of necessary parts, and services based on the design, assembly, processing, and delivery of final products and services. It was deployed in a fixed and unchanging manner. In contrast, the CPS, where cyberspace and physical space are highly integrated, requires that goods and services be provided to the people who need them when they need them. The starting point for a series of activities to create added value is not fixed. In the past, suppliers planned and designed the added value; from now on, there will be an increasing number of cases where customers will become the starting point for creating added value. These activities may change during the process owing to changes in the requirements specified when starting the creation of added value. If more effective and accurate data are obtained, these elements are incorporated into new activities.

The IEC TR Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment show five critical concepts for cybersecurity and resilience for smart energy by highlighting the convergence between IT and OT, as shown by Figure 5.

Figure 5: Five Concepts for Cyber System Security in the IEC



Source: IEC TR Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment.

Concept 1: Resilience should be the overall strategy for ensuring business continuity. When focusing on resilience in general, organisations must consider the safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent) but also during incidents (detect and respond) and after incidents have been resolved (recover). For the resilience of cyber assets, organisations must similarly consider safety, security, and reliability for cyber assets. Resilience thus involves a continuous improvement process to support business continuity. It is not just a technical issue but must involve an overall business approach that combines cybersecurity techniques with system engineering and operations to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Information sharing within and across organisations is also becoming crucial as a part of resilience.

Concept 2: Security by design is the most cost-effective approach to security. Security is vital for all critical infrastructures and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented. This means that the products, systems, processes, and organisation should be designed or set up from the beginning with security in mind. However, recognising that security cannot easily be added to legacy systems, particularly since system components may have different life cycles, it is crucial that even for these existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades. Security by design combines business organisational policies with security procedures and supportive technologies. Organisational policies include security regulations, personnel training, and segregation of duties, whilst security procedures include a computer emergency response team, information sharing, backup and recovery plans, and secure operations. Security technologies include physical and logical techniques, such as physical site access locks, access control, authentication and authorisation for all communications, and security logs.

Concept 3: IT and OT are similar but different. Technologies in operational environments (referred to here as OT) have many differing security constraints and requirements from IT environments. The primary reason is that the power system is a CPS, and security incidents can cause physical safety and/or electrical incidents, whereas such physical consequences are not usually a problem in corporate environments. For IT environments, the confidentiality of sensitive business and customer information is usually the most important requirement, but for OT environments, the availability, authentication, authorisation, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive. At the same time, the OT environment is increasingly relying on cyber technologies and is inheriting more and more devices and platforms from the IT world, whilst both IT and OT environments are increasingly converging on the use of well-known and ever-evolving Internet of Things (IoT) technologies. This interconnection between IT and OT and increased dependence on IoT technology are leading to additional vulnerabilities and challenges in ensuring adequate security in the energy environment. Therefore, the selection of appropriate security measures has focused on the security requirements as determined by risk assessment.

Concept 4: Risk assessment, risk mitigation, and continuous updating of processes are fundamental to improving security. Based on an organisation's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, and reputational) for all its business processes. Risk assessment identifies the vulnerabilities of systems and processes to deliberate or inadvertent threats, determines the potential impacts, and estimates the likelihood that the incident scenarios could actually occur. Strategies for risk mitigation must take into account operational constraints, as well as look to engineering designs and operational procedures to improve resilience whilst also evaluating the cost of implementing such a potential risk mitigation strategy and the degree to which it mitigates risk. Risk assessment also requires that mitigation processes be re-evaluated during regular periodic security reviews or triggered by actual security incidents.

Concept 5: Cybersecurity standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programmes and policies. Cybersecurity measures should not be reinvented. Key cybersecurity standards and best practice guidelines have already been developed for different areas and purposes of security. Cybersecurity planning should use these cybersecurity standards and guidelines to improve the resilience and security of the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

2.2. Security Design in A Cyber-physical System

In a CPS, cyberspace and physical space are highly integrated. Cyberspace expands drastically, and points of cyberattack expand. The two spaces interacting with each other increase the impact of the damage on physical space. Threats to a CPS are different and more complex compared to the linear supply chain model and will cause a wider range of damage. It is a major change that the threat of cyberattacks has expanded as the number of attacked points has increased. For this reason, it is necessary to have measures to ensure security in all the elements and to ensure the trustworthiness of the entire process in the CPS through comprehensive measures, not partial ones. In addition, new processes will occur with the advanced integration of cyberspace and physical space, such as the digitisation of information obtained from IoT, and the exchange of a large amount of created data is emerging as a new target for cyberattacks. This needs to be recognised, and ensuring the security of the digitalisation of information and security measures to support the accuracy, distribution, and coordination of a large amount of data will become important issues. Table 1 shows the features of a CPS in the Cyber/Physical Security Framework (CPSF).

Table 1: Features of Cyber-physical System

A large quantity of data exchange	• Appropriate management suited to the characteristics of the data is becoming increasingly important
Integration of physical space and cyberspace	• Cyberattacks reach physical space • Intrusions from physical space and attacks on cyberspace are assumed • Interventions in the process of information conversion between physical space and cyberspace are assumed
Complexity of supply chain connections	• Range affected by cyberattacks expands

Source: Ministry of Economy Trade and Industry, the Japanese government (2019a).

2.3. The Security Triangle of Implementation, Regulation, and Framework

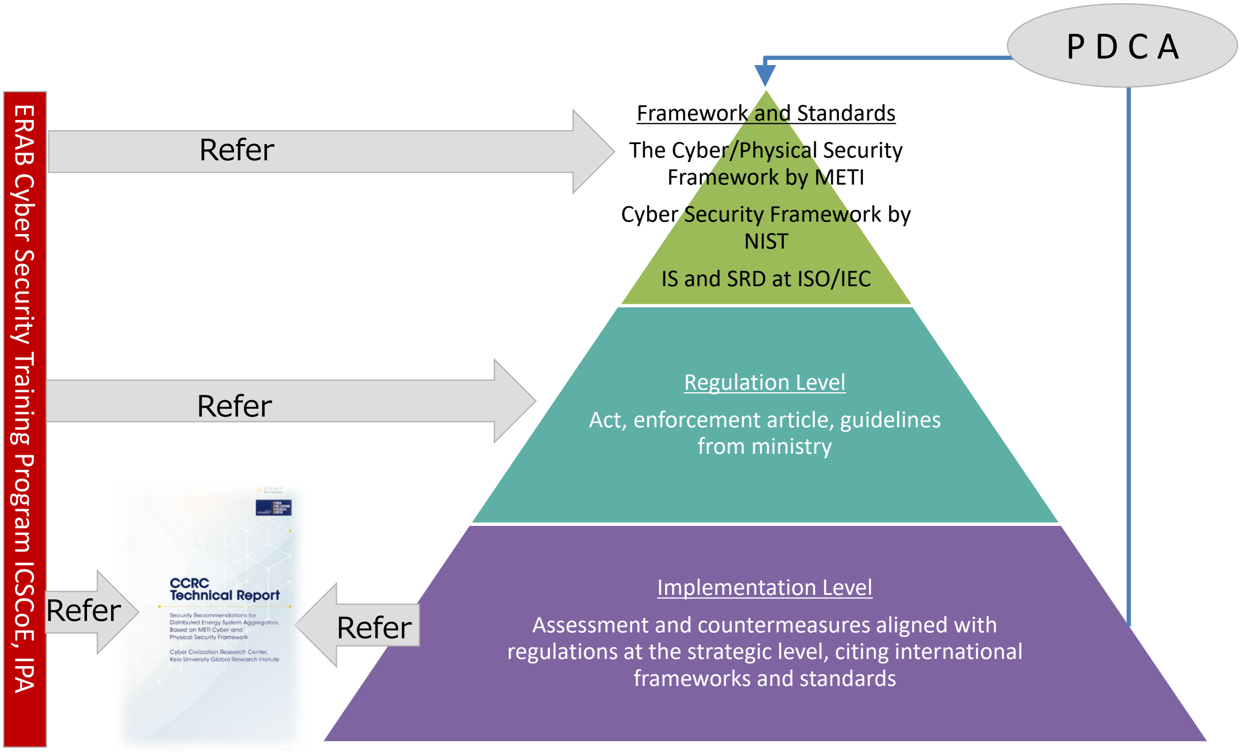
The most important part of ERAB, in which physical and cyber spaces are connected to the Internet, is to create trustworthiness in cyber-physical systems. To achieve security for ERAB, it is necessary to have a security triangle using the three layers of implementation, regulation, and framework, as shown in Figure 6. Specifically, it is important to formulate specific guidelines for each country that are in line with the DES and ERAB businesses that are subject to the regulation level, formulate guidelines that embody these at the implementation level, and reflect them in the evaluation of security measures and appropriate operations. From the viewpoint of security by design, it is important to refer to frameworks such as the CPSF and international standards such as IEC standards. In addition, the Plan, Do, Check, Action cycle involves implementing cybersecurity measures at the implementation level, reviewing them, and then feeding the results back into updating the guidelines at the regulatory level and standards.

Thus, Japan has achieved even more robust but feasible cyber and physical system security measures. The Japanese experience instructs the system to have reliable frameworks before tailoring them to specific circumstances in each country. Incorporating regional characteristics and enhanced cooperation in sharing country-specific experiences will contribute significantly to the development of more resilient and effective cyber and physical system security mechanisms across Association of Southeast Asian Nations (ASEAN) countries.

When establishing a Plan, Do, Check, Action cycle, it is necessary to understand that actual operations are affected by the local context. Sharing experiences based on the evidenced-based approach[2] (EBA), including sharing attack scenarios that are generated through security assessments in accordance with ISO 31000 and IEC 27000 for basic standards and CPSF for more detailed guidance, will contribute to the quality development of the security triangle for ERAB in ASEAN, as shown in Figure 6.

[2] SOI Asia, which promotes academic Internet research, operations, and education in collaboration with universities across Asia, is introducing the EBA as an educational method applicable to artificial intelligence (AI) and data science. More information is available at https://eba.soi.asia/

Figure 6: Security Triangle for a Cyber-Physical System


P D C A
ERAB Cyber Security Training Program ICSCoE, IPA
Refer
Refer
Refer
Refer
Framework and Standards
The Cyber/Physical Security Framework by METI
Cyber Security Framework by NIST
IS and SRD at ISO/IEC
Regulation Level
Act, enforcement article, guidelines from ministry
Implementation Level
Assessment and countermeasures aligned with regulations at the strategic level, citing international frameworks and standards
CCRC Technical Report
Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework
Cyber Civilization Research Center, Keio University Global Research Institute

Source: Authors.

Risk analysis for cyber-physical systems by the CPSF

The Cyber/Physical Security Framework (CPSF), published by the Japanese government's Ministry of Economy, Trade and Industry, shows a model that appropriately identifies the risks faced in creating added value and risk sources, organising an overview of the required security measures and summarising examples of measures in a CPS. The CPSF covers all entities working to create added value in the CPS. It identifies risk sources and security measures as:

- those applicable to conventional supply chains, and
- those that need new measures in the new industrial society model.

The CPSF adopts a three-layer, six-element model for its analysis.

2.4. The First Layer: Connections between Organisations

The first layer aims to ensure trust in the organisation's management. This approach has been adopted to achieve security across supply chains. This is based on the idea that security can be assured by verifying the trustworthiness of enterprise management and accepting only participants whose trustworthiness is known. Certification programmes, such as the Information Security Management System (based on ISO/IEC 27001), focus on confirming trust in company management (divisions and headquarters) and provide a mechanism that leads to connections between companies that can be trusted to support security in the supply chain. Using this approach, security policies are shared, and the trustworthiness of the management is verified and certified. In summary, the first layer aims to implement shared and certified security policies as a basis for promoting trust. In an industrial society, however, where cyber and physical spaces are integrated, it is impossible to ensure trust throughout the entire value creation process by confirming the trustworthiness of the organisation's management. Therefore, the second and third layers of the model introduce more advanced methods focused on the value-creation process.

2.5. The Second Layer: Connections between Cyberspace and Physical Space

As IEC TR 62351-12:2016 presents, DERs should be designed to assume that breaches will in fact occur and that their impact will be both minimal and within the design tolerances for the overall DER mission. This is particularly important because breaches of DER security could disrupt the broader energy grid, with consequences such as the exposure of information related to consumers, such as their location and when their homes are vacant.

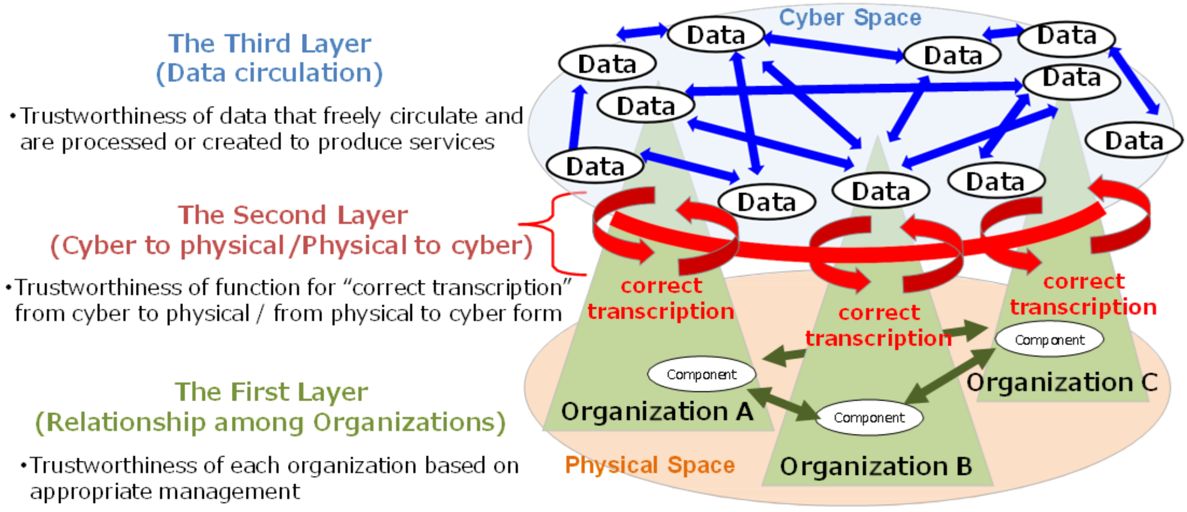
DERs in ERAB systems seek to connect everything to the network and create borders between cyberspace and physical space. The connections between cyber and physical spaces are found in many industrial and social activities. However, unreliable interactions between cyberspace and physical space can cause uncertainty in industrial society. The value-creation process expands over the border between cyberspace and physical space. Trustworthiness cannot be safeguarded if information accuracy cannot be relied on. The value creation process requires interaction between cyberspace and physical space to achieve high accuracy. In other words, the trustworthiness of the value-creation process must confirm the accuracy of transcription and translation.

The second layer is based on the accuracy and trustworthiness of data transcription and transfer (including accurate translation) between cyberspace and physical space. The IoT system's actual border between cyberspace and physical space comprises sensors that translate physical events (e.g. temperature, humidity, and distance) into data, resulting in actionable events. The security of systems that transfer data on the border between cyberspace and physical space cannot be safeguarded by confirming the trustworthiness of the organisation's management. To ensure trustworthiness in transcription, in accordance with ISO/IEC 27036, all elements of the system life cycle, including construction and maintenance, must also be trustworthy. Another point to be understood is that the existing systems will be incorporated into the new frontier between cyberspace and physical space. Therefore, it is important to regularly (and ideally continually) evaluate system security and take measures to ensure the security of the transcription functions.

2.6. The Third Layer: Connections in Cyberspace

As the quantity of data drastically increases in an industrial society, creating new value in cyberspace through data exchange and analysis has become commonplace. The trustworthiness of the data transcribed from the physical space to cyberspace is promoted by ensuring the trustworthiness of the transcription function in the second layer. However, it should be noted that data are created, edited, processed, and freely exchanged in cyberspace outside the second-layer process, not only by organisations with known trustworthiness. Although many entities may use and modify a dataset, the original data create value in cyberspace. In cyberspace, to ensure the trustworthiness of the value creation process and to create value as intended, data must invite trust. Therefore, in the third layer, data integrity is the basis for trustworthiness. Data falsification and breaches during the distribution and storage of data will lead to a loss of trust in the entire value-creation process. Therefore, security measures need to be implemented in the third layer for data distribution and storage, and appropriate editing and processing. In summary, in the value-creation process of an industrial society where cyberspace and physical space are highly integrated, security measures from all three layers are required. Risk sources were identified using a three-layer model.

Figure 7: Three Layers of Industrial Society


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
Cyber Space
Data
correct transcription
Component
Organization A
Organization B
Organization C
Physical Space

Source: Ministry of Economy Trade and Industry (2019a).

2.7. Six Elements

This section explains the six elements in the CPSF.[3] First, it is necessary to understand that the elements of the value-creation process should be considered separately because the process is organised dynamically and flexibly. Therefore, it is challenging to grasp fixed business assets. In the CPSF, the elements are the organisation, people, components, data, procedure, and system (Table 2).

Table 2: Six Elements of Trustworthiness Creation in CPSF

Element	Definition
Organisation	Companies, groups, and organisations that comprise the value creation processes
People	People belonging to organisations, 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, analysing, and simulating it
Procedure	Sequences of activities to achieve the defined purpose
System	Mechanisms or infrastructures configured with components for the defined purpose

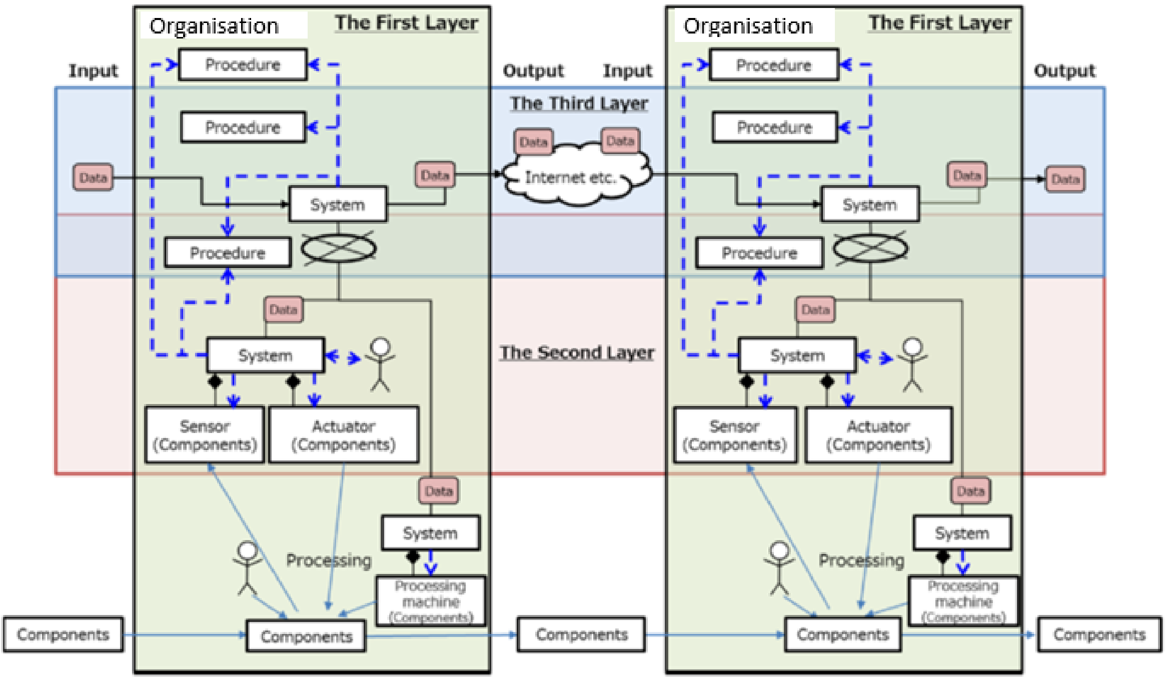
Source: Cyber/Physical Security Framework (CPSF).

2.8. Map ERAB to the Three-layer and Six Elements Model in the CPSF

The risk sources in ERAB will be identified, and associated policies will proceed through the risk assessment, for which the three-layer and six-element model is applicable. As an example of the value-creation process in the manufacturing industry, the relationship between the three layers and six elements is shown in Figure 6. Within each organisation, there is a flow of components, such as inputs and outputs of processing machines, sensors, actuators, systems that exchange data with other organisations, people who monitor and control the systems, and procedures that establish each system activity, including software and various types of data that flow between systems. First, the organisation receives components – that is, inputs – processes them, and creates output components, which are then input to another organisation that performs additional processing and creates new output components.

[3] For more details, see 'Part I (Concept): Industrial Cyber Security for Connected Cyber and Physical Systems' in the CPSF. The CPSF is available at https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf

Figure 8: Relationship between the Six Elements in the Three-layer Model



Source: Cyber/Physical Security Framework (CPSF).

Each organisation's components constitute the first layer of the company. Amongst the elements of the first layer, sensors and actuators translate between cyberspace and physical space, the systems controlling them, and the related procedures. The data are organised as second-layer elements. Finally, between the two organisations, the data are exchanged via the Internet and the related systems and procedures and organised as the elements of the third layer that connect in cyberspace.

These six elements do not have exclusive relationships with one another. For example, the organisation element comprises other elements, such as people, systems, and/or procedures. However, the organisation also has the meaning of the original element in the value-creation process. People are not only an element in the organisation but also directly participate in the value-creation process. The trustworthiness of the value-creation process is secured by taking security measures against risk sources in an attempt to compromise the six elements in the value-creation process. Thus, the trustworthiness of the created hardware, software, and services is ultimately secured.

One of the essential features of a DER system is the tight coupling of cyber systems and the physical world. In the CPSF, the second layer, that is, the mutual connections between cyberspace and physical space, is highlighted. Many of these systems, such as IoT servers, are mission-critical and cannot be shut down. A traditional security rescue solution is required to shut down the system to perform maintenance and remove different types of viruses or malware from the server, roll it back to a known prior state, and then restart. However, this recovery approach cannot be applied to mission-critical DER systems that are single points of failure. Cybersecurity challenges are yet to be solved, but additional security risks and problems can emerge owing to the integration of these DER systems.

2.9. Trustworthiness in the ERAB system

According to the understanding that ERAB systems are cyber-physical systems, DER products and services are created in different countries and regions that make up the global supply chain, and there is a need to ensure the trustworthiness of ERAB systems. The CPSF aims to make progress in this area. The security needs of physical data produced by DERs – and their digitisation, transport, storage, and analysis – differ from the interactions between two trusted entities in a conventional supply chain. DER data are often used to generate new data through automated analyses. The data are also used to create physical products and services in the physical space by controlling the physical DERs. All of these interactions must be secured and managed through the participants' value-creation process.

The security of the entire value-creation process is ensured by each entity securing each element, which is the basis of trustworthiness based on the three layers. The CPSF shows the management process of trustworthiness: it is necessary to confirm that each element's security requirements are satisfied (creation of trust), enquired by other subjects except the subject of confirmation (proof of trust), structure, and maintaining a chain of trustworthy relationships (trustworthy chain) built up in a chain by repeating creation and proof of trust. Examples of matters required to create trust, proof of trust, and structuring and maintaining a trustworthy chain are shown below.

Creation of trust

i. Examples
   - Create components/data that satisfy security requirements.
   - Preserve the aforementioned records.
   - Self-confirmation of the components/data being created with satisfied security requirements.
   - Third-party certification that the components/data have been created with satisfactory requirements.

Proof of trust

ii. Examples

- Creating and managing a list (for trustworthiness) that can be inquired by third parties other than the production subject, ensuring that the target components/data are properly created in a form that satisfies security requirements, regardless of whether it is an integrated ledger or a distributed ledger (such as blockchain).
- Confirming the trustworthiness of the target components/data.

Structuring and maintaining of trustworthy chain

iii. Examples

- Structuring a trustworthy chain through repeated creation and certification of trustworthiness (each chain element’s trustworthiness is confirmed against other elements, thereby securing traceability).
- Detection of/protection against external attacks on a trustworthy chain.
- Improvement in resilience to attacks.

3. Conclusion: Common Understandings Towards Energy Transition

3.1. ERIA Study Group on Cyber and Physical System Security of DERs

In October 2024, the Economic Research Institute for ASEAN and East Asia (ERIA) launched a study group on cyber and physical system security for distributed energy resources (DERs), in alignment with the Asia Zero Emission Community (AZEC). The group was established in response to the following background and objectives:

Background:

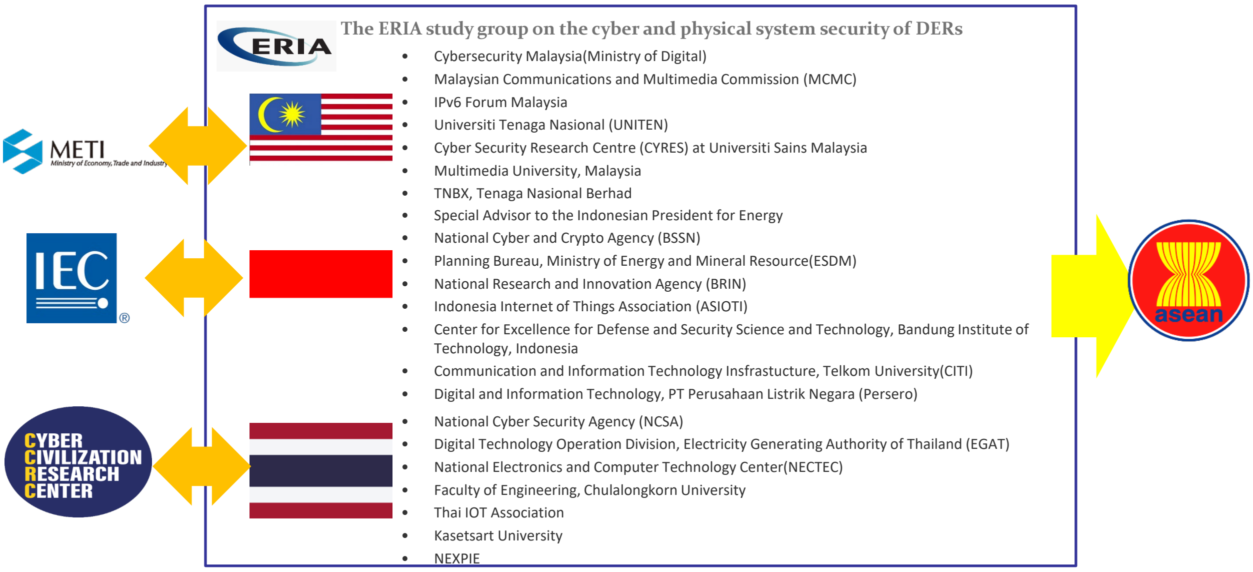
Rapid economic growth in Southeast Asia has led to a significant increase in energy demand. To support continued development and achieve sustainable growth, the region must pursue both energy security and the decarbonisation of its energy systems. Distributed energy systems (DESs) – such as renewable energy technologies and smart grids – are expected to contribute to both objectives. However, as these systems rely on IoT-enabled devices and are connected to broader networks, they are increasingly vulnerable to cyber threats. This makes it essential to consider robust cybersecurity frameworks for DESs.

Objectives:

1. To clarify the current status of DES deployment and cybersecurity in the energy sector;
2. To develop a basic concept for promoting cybersecurity for DESs;
3. To foster a shared understanding of this concept amongst key stakeholders.

The study group included regulatory authorities, industry professionals, and academic experts from both ASEAN and Japan, as illustrated in Figure 9.

Figure 9: The ERIA Study Group on the Cyber and Physical System Security of DERs



The ERIA study group on the cyber and physical system security of DERs

- Cybersecurity Malaysia(Ministry of Digital)
- Malaysian Communications and Multimedia Commission (MCMC)
- IPv6 Forum Malaysia
- Universiti Tenaga Nasional (UNITEN)
- Cyber Security Research Centre (CYRES) at Universiti Sains Malaysia
- Multimedia University, Malaysia
- TNBX, Tenaga Nasional Berhad
- Special Advisor to the Indonesian President for Energy
- National Cyber and Crypto Agency (BSSN)
- Planning Bureau, Ministry of Energy and Mineral Resource(ESDM)
- National Research and Innovation Agency (BRIN)
- Indonesia Internet of Things Association (ASIOTI)
- Center for Excellence for Defense and Security Science and Technology, Bandung Institute of Technology, Indonesia
- Communication and Information Technology Insfrastucture, Telkom University(CITI)
- Digital and Information Technology, PT Perusahaan Listrik Negara (Persero)
- National Cyber Security Agency (NCSA)
- Digital Technology Operation Division, Electricity Generating Authority of Thailand (EGAT)
- National Electronics and Computer Technology Center(NECTEC)
- Faculty of Engineering, Chulalongkorn University
- Thai IOT Association
- Kasetsart University
- NEXPIE

ERIA
METI
Ministry of Economy, Trade and Industry
IEC
CYBER CIVILIZATION RESEARCH CENTER
asean

Source: Authors.

3.2. Common Understanding in the Study Group

Ongoing discussions within the study group have led to a shared understanding of the key principles needed to navigate the energy transformation pathway toward carbon neutrality:

- **Advance the energy transition through decarbonisation, decentralisation, and digitalisation.** The Energy Resource Aggregation Business (ERAB) represents an advanced model that applies distributed energy resources (DERs) to provide new energy service scenarios tailored to local demand. It leverages open-standard technologies to encourage new market entrants and innovation.
- **Apply a security-by-design approach to ERAB, as a cyber-physical system (CPS).** The Cyber/Physical Security Framework (CPSF) is essential for securing CPSs such as ERAB.
- **Ensure robust security design within CPSs.** Because successful cyberattacks can result in physical harm, security is a fundamental safety concern, not merely an issue of data protection.
- **Design security measures with interoperability in mind.** Security solutions must not hinder the critical data sharing and coordination needed for system functionality.

- **Recognise the growing interdependence of critical infrastructures,** which introduces new and emerging risks.
- **Support system resilience and stakeholder coordination.** Distributed energy systems (DESs), the backbone of ERAB, manage diverse stakeholders and enable system redundancy, which has been key to the success of the Internet.
- **Prioritise data accuracy.** For example, mitigating GPS jamming through alternative technologies is essential to support high-quality AI and automation.
- **Promote international collaboration.** Achieving net-zero emissions under the Asia Zero Emission Community (AZEC) framework will require cross-border co-operation. Examples include the Indonesian government's decarbonisation initiatives and Japan's Global South Future-Oriented Co-Creation Project.

Despite its potential, ERAB remains vulnerable to security risks that limit its full-scale, trustworthy deployment. The decentralised nature of DERs exacerbates challenges in establishing trust and verifying the authenticity of participating devices. Furthermore, the absence of clearly defined roles, responsibilities, and accountability mechanisms within the ERAB ecosystem contributes to fragmentation and potential insecurity.

A lack of standardised security protocols also impairs interoperability and secure communication amongst system components. Many existing DER protocols lack embedded security features, making them susceptible to a range of cyberattacks, including:

- **Eavesdropping:** Interception of communications, compromising sensitive data.
- **Unauthorised access:** Attackers taking control of devices to manipulate energy flows.
- **Data tampering:** Alteration of information that could affect billing accuracy, system stability, and safety.
- **Replay attacks:** Reuse of captured messages to disrupt system operations.
- **Denial-of-service (DoS) and Economic Denial of Sustainability (EDoS) attacks:** Disruption of service availability and undermining of ERAB's economic viability.

3.2.1. The Necessary Approach: Mapping the CPSF to ERAB in a Laboratory-Scale Test Bed

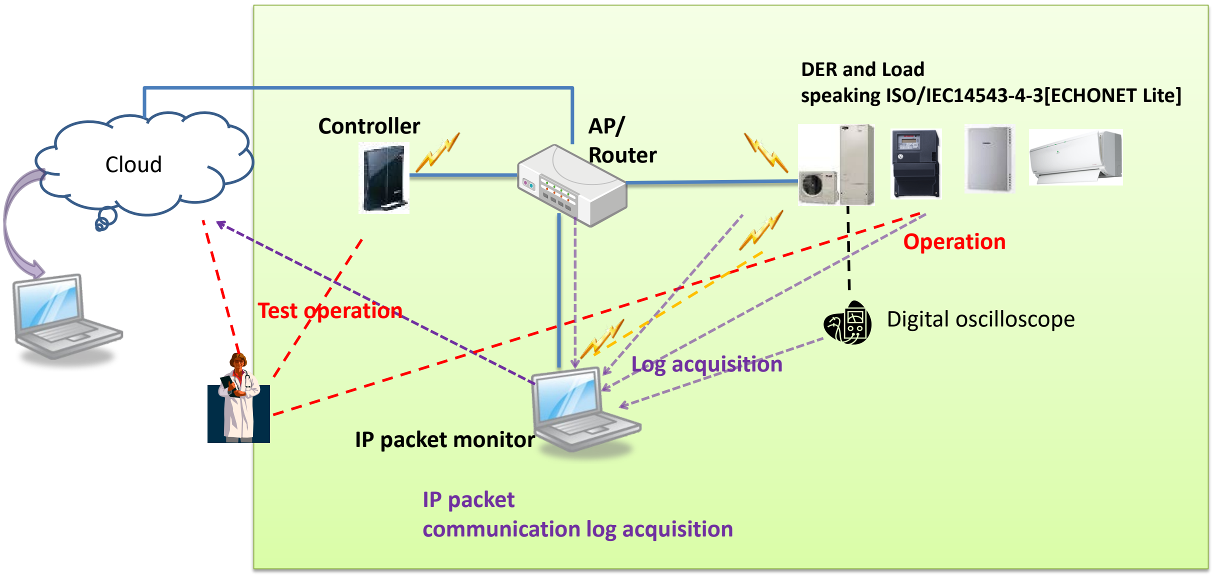
To enable a trusted energy transition and establish the ERAB 'security triangle' – comprising implementation, regulation, and framework – it is essential to map the

Cyber/Physical Security Framework (CPSF) to ERAB. This approach helps identify emerging threats influenced by local contexts.

A laboratory-scale test bed plays a critical role in conducting penetration testing, which is vital for developing and maintaining both cyber and physical security systems. Sharing insights from test results in ASEAN and Japan – such as experiences in implementing the ERAB security triangle – is fundamental to fostering international co-operation.

The test bed enables simulation of attack scenarios in near real-world conditions, providing a controlled environment for testing DERs. These DERs are equipped with open and internationally standardised interfaces, such as ECHONET Lite (IEC14543-4-3), and have Internet connectivity, as illustrated in Figure 10.

Figure 10: A Laboratory-scale Test Bed



Source: Authors.

3.2.2. *Expected Actions and Deliverables Towards 2025–2026*

To design and evaluate a comprehensive trust framework for ERAB that incorporates open-standard technologies, the following actions are proposed:

A) Design a service that ensures trustworthiness amongst device communications in a distributed system.

The Centralised Discovery Service (CDS) will provide:

- **Controlled access:** Ensuring that only authorised devices and entities can participate in the ERAB ecosystem.
- **Robust authentication and authorisation:** Implementing mechanisms to verify identities and assign appropriate access privileges.
- **Secure device registration and management:** Establishing a centralised system to manage device credentials and maintain an up-to-date registry of trusted devices.

B) Define trustworthiness and accountability.

The ERAB 'security triangle' outlines necessary security actions to build a framework for trust and accountability within the ERAB ecosystem:

- **Define roles and responsibilities:** Clearly assign obligations to stakeholders, including energy companies, aggregators, consumers, and regulatory bodies.
- **Establish accountability measures:** Develop procedures for addressing security breaches and privacy violations, including incident response protocols and potential penalties.
- **Ensure transparency:** Require the disclosure of any cyberattacks or data breaches to all relevant ERAB stakeholders.

C) Build a community of experts.

Engage researchers, academics, industry professionals, and policymakers to collaboratively design and implement CPS security policies.

The ERAB ecosystem can contribute significantly to realising the energy transition by supporting a secure, efficient, and resilient infrastructure – key principles of the CPSF. The expected deliverables are:

A) A policy framework aligning national cybersecurity priorities with regional energy governance, offering regulatory guidance tailored to local contexts.

B) Technical standards and operational procedures based on multilayered risk mapping of subsystem components within the Smart System 4-Layer architecture.

C) A role-based education and training platform to raise awareness, enhance preparedness, and build capacity to manage cyber-physical threats.

D) Tangible outputs such as a white paper, academic research papers, or a national roadmap for CPS security.

E) A detailed analysis of the electricity market structure, including current generation, distribution, technologies, policies, and business mechanisms – highlighting challenges that hinder DER integration.

F) A comprehensive evaluation of ERAB feasibility, including:

1. An assessment of technical readiness, economic implications, regulatory gaps, and stakeholder dynamics in the shift from centralised to decentralised energy systems.
2. A CPSF-compliant DER system architecture design.
3. An integrated architecture that supports DER deployment aligned with CPSF principles – emphasising cybersecurity, privacy, interoperability, and resilience.

This study offers a timely and critical investigation into the evolving security and privacy challenges of ERAB ecosystems. By developing a comprehensive trust framework, it supports the secure and reliable deployment of smart-grid technologies, advancing sustainable energy management and enhancing consumer trust. The proposed methodology – combining theoretical insight, design science, and rigorous evaluation – ensures robust and practical outcomes. These deliverables will be valuable to energy providers, technology developers, policymakers, and researchers alike, paving the way for a secure and trustworthy energy future.

3.2.3. The Necessary Philosophy to Balance Openness and Security

The expert group recognises that the value of open technology is equal to the risks it presents in terms of threats and vulnerabilities. Striking the right balance between openness and security is essential.

The evolution of the Internet – an enabler of telecom network transformation – demonstrates that its success lies in open-standard, autonomous, distributed, and globally governed systems that accommodate diverse stakeholders and incorporate redundancy.

Yet, the most important element of implementing security through the design of cyber-physical systems to drive energy transformation is a guiding philosophy that bridges research and real-world implementation. As Dr Jun Murai, known as the 'father of the Internet' and a member of the Internet Hall of Fame, stated:

'Research on our left hand, operation on our right hand. Support social infrastructure with both hands.'

This dual commitment to research and operational excellence must be central to energy security strategies going forward.

References

International Electrotechnical Commission (2024), *Committee draft: Distributed Energy Resource Aggregation Business System: Architecture and Service scenario, System committee smart energy*, Geneva: IEC.

International Electrotechnical Commission (2019), T*echnology report: Cyber security and resilience guidelines for the smart energy operational environment, System committee smart energy*, Geneva: IEC.

Umejima, M., S. Manickam, C.P. Metcalfe, D. Farber, J. Murai, J. Kokuyo, and C. Wong (2021), 'Security Recommendations for Distributed Energy System Aggregators, based on METI Cyber and Physical Security Framework', CCRC Technical Report, Keio University, Tokyo: KEIO.

Ministry of Economy Trade and Industry, the Japanese government (2019a), *Cyber/Physical Security Framework (CPSF)*. Tokyo: METI.

Ministry of Economy Trade and Industry, the Japanese government (2019b), *Cybersecurity Guidelines for Energy Resource Aggregation Business Ver 2.0*. Tokyo: METI.

ERIA Discussion Paper Series

No.	Author(s)	Title	Year
2024-04 (No. 550)	Junianto James Losari	Compliance Analysis of Indonesia's LCR Measures: International Trade and Investment Agreement Perspectives?	July 2025
2024-03 (No. 549)	Venkatachalam Anbumozhi, Kaliappa Kalirajan, Ayu Pratiwi Muyasyroh, Veerapandian Karthick	Putting a Price on Carbon in ASEAN and East Asia: Are Consumers Willing to Pay?	May 2025
2024-02 (No. 548)	Bhupendra Kumar Singh, Venkatachalam Anbumozhi, Rakesh Kumar Agarwal	India-ASEAN Power Trading and Regional Grid Connectivity: Status, Challenges, and Policy Innovations Required for Acceleration	May 2025
2024-01 (No. 547)	David Christian and Lili Yan Ing	Trajectory of Southeast Asian Production Fragmentation	May 2025
2024-39 (No. 546)	Sanja Samirana Pattnayak	Digitalisation, Exports, and Firm Performance: A Case of Indian Manufacturing	March 2025
2024-38 (No. 545)	Ju Hyun Pyun and Jong-in Sun	Global Pandemic Shocks, Foreign Exposure and Firm Productivity: Evidence from Korean Firm-level Data	March 2025
2024-37 (No. 544)	Abhishek Kumar, Apra Sinha, and Gazi Salah Uddin	Revenue and Cost Uncertainties and Market Power	March 2025
2024-36 (No. 543)	Md Lutfur Rahman and Sudipta Rose	Firm-level Climate Vulnerability and Corporate Risk-taking: International Evidence	March 2025
2024-35 (No. 542)	Alloysius Joko Purwanto, Ridwan Dewayanto Rusli, Hafis Pratama Rendra Graha, Sirichai Koonaphapdeelert, Reza Miftahul Ulum, Citra Endah Nur Setyawati, Nadiya Pranindita, Ryan Wiratama Bhaskara	Carbon Emission Reduction Potential of Hydrogen Production for Large-Scale Industrial Facilities in Southeast Asia	February 2025

ERIA discussion papers from previous years can be found at:

http://www.eria.org/publications/category/discussion-papers