Research on the Introduction and Pilot Implementation of IEC 62443 Standard in Microgrid Fields

ICT Research Laboratory: Lin Cheng-Hung, Kuo Jia-Hong

1. Research Background

With the advancement of energy transition, the increase in penetration of renewable energy into the grid, and the rapid proliferation of distributed energy resources, microgrids have become an important technology for enhancing the resilience, stability, and dispatching flexibility of power systems. A microgrid integrates solar photovoltaic systems, energy storage systems, power conversion equipment, sensing devices, human-machine interfaces, and centralized control systems supporting energy management, control strategy validation, and power supply resilience testing. However, microgrids also lead to a high degree of integration between traditional power equipment and information and communication technologies, exposing the operational technology environments to more complex cybersecurity risks.

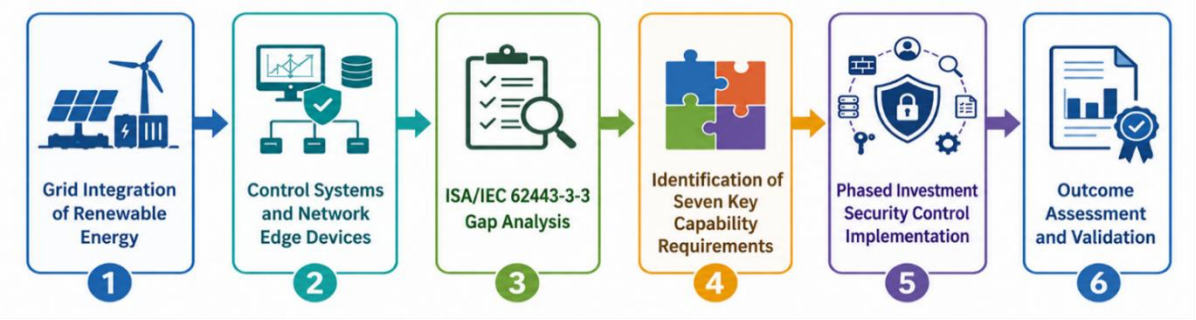
Unlike in general information systems, cybersecurity incidents in microgrid control systems may not only result in data leakage or service interruption, but may also affect power dispatching, equipment start-stop operations, energy storage charging and discharging control, and on-site operational safety. Therefore, cybersecurity protection should not focus solely on individual devices or network nodes. Instead, it should be examined at the system level, covering capabilities such as identification and authentication, access control, data flow restriction, event logging, integrity protection, data confidentiality, and resource availability.

This study focuses on the Shulin Microgrid Integration Verification Site. The site includes actual equipment, real communication behaviors, and personnel operation scenarios, allowing it to reflect cybersecurity issues encountered in real microgrid operations, such as control interface access, cross-system data exchange, boundary communication governance, and long-term maintenance configuration consistency. To ensure consistency, traceability, and verifiability in cybersecurity implementation, this study adopts ISA/IEC 62443-3-3 as the basis for system-level cybersecurity assessment and enhancement. Security Level 1 (SL1) is set as the implementation target for this stage. Through gap analysis, risk identification, conversion of control requirements, and phased implementation, a sustainable and improvable certification pathway is established.

2. Research Results

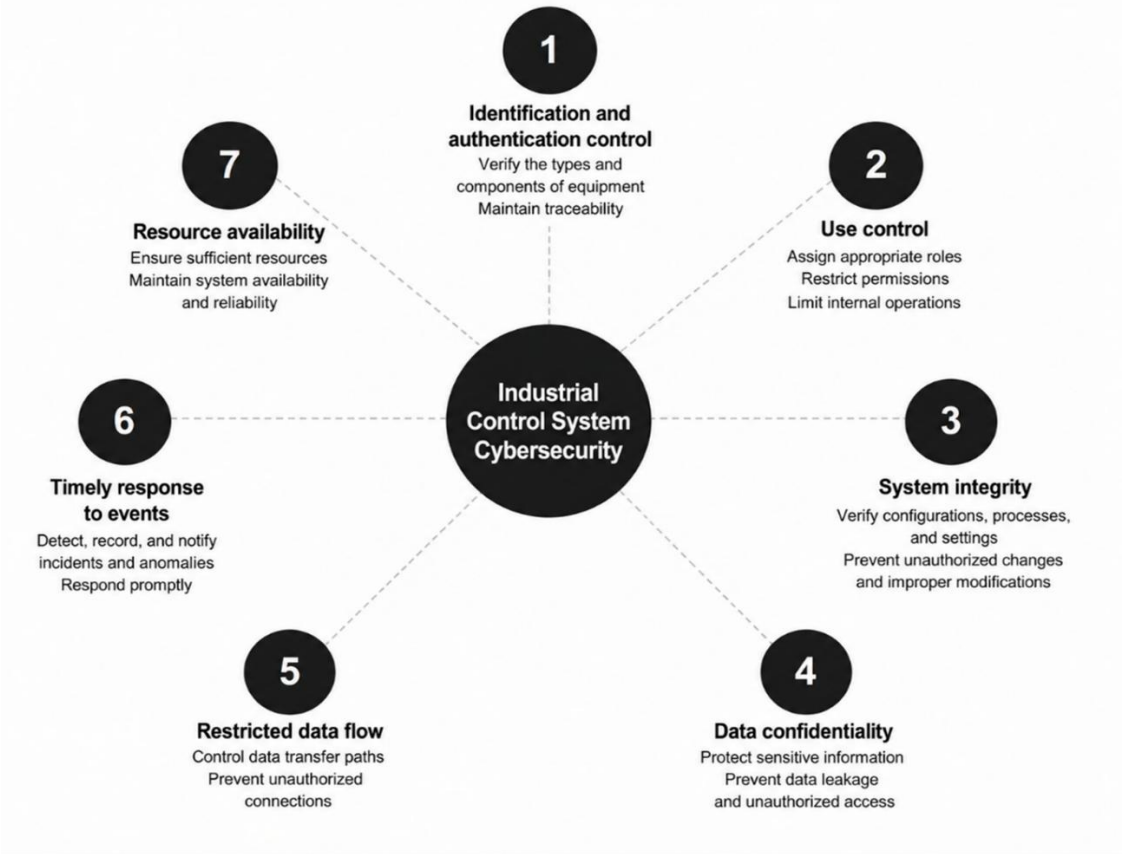
To achieve ISA/IEC 62443-3-3 SL1 certification, this study established a certification workflow as illustrated in Figure 1. A systematic inventory was conducted for control systems and network boundary protection components. The analysis scope covered the seven Foundational Requirements (FR): Identification and Authentication Control (IAC), Use Control (UC), System Integrity (SI), Data Confidentiality (DC), Restricted Data Flow (RDF), Timely Response to Events (TRE), and Resource Availability (RA), as shown in Figure 2. Each requirement was benchmarked against current system functions, configuration states, and actual operational scenarios, categorized into three types: "Achieved," "Not Achieved," or "Not Applicable."

Descriptions of the comparison results and recommendations for improvement were provided, enabling the research team to clearly understand the current maturity and primary sources of gaps. The preliminary results are summarized in Table 1.



Source: Compiled by this research

Figure 1. Compliance Framework for IEC 62443 Implementation in Microgrid Environments



Source: Compiled by this research

Figure 2. Seven Foundational Requirements

Table 1. Preliminary Results of ISA/IEC 62443-3-3 Gap Analysis

Requirement family	Total	Achieved	Not achieved	N/A
Identification and authentication control	10	9	0	1
Use control	8	5	1	2
System integrity	5	1	3	1
Data confidentiality	2	0	2	0
Restricted data flow	4	3	0	1
Timely response to events	1	1	0	0
Resource availability	7	3	4	0
Total	37	22	10	5

Source: This research

The preliminary gap analysis results showed that among the 37 system-level security requirements, 22 had already been achieved, 10 had not yet been achieved, and 5 were not applicable. The system had already established fundamental capabilities in areas such as identification, login authentication, account management, password complexity, login failure lockout, privilege classification, session locks, and log management. However, there remained room for improvement in system integrity, data confidentiality, event management, input validation, zone and conduit modeling, and resource availability.

Subsequent improvements were implemented based on the gap analysis results, including strengthening the protection of authentication information, communication integrity, network segmentation, boundary control, event logging, access control for audit records, asset inventory, and configuration management. Unnecessary communication paths were gradually reduced, and a clearer zone and conduit model was established. Ultimately, all previously unachieved requirements were successfully addressed, as shown in Table 2, and the ISA/IEC 62443-3-3 SL1 certificate was obtained.

Overall, this study completed the full implementation process for the microgrid site, from current-state inventory and gap identification to improvement

implementation and certification completion. It established a practical and feasible methodology for strengthening industrial control system cybersecurity. This certification pathway can serve as an important reference for the company in evaluating manpower, resources, costs, and implementation steps when introducing ISA/IEC 62443-3-3 SL1 in the future.

Table 2. Final Implementation Results of ISA/IEC 62443-3-3 Security Controls

Requirement family	Total	Achieved	Not achieved	N/A
Identification and authentication control	10	9	0	1
Use control	8	6	0	2
System integrity	5	4	0	1
Data confidentiality	2	2	0	0
Restricted data flow	4	3	0	1
Timely response to events	1	1	0	0
Resource availability	7	7	0	0
Total	37	32	0	5

Source: This research