Grid-Side Communication Requirements for Small Modular Reactors as Ancillary Service Providers in the Smart Grid

Ebru Ekici Güngör
Department of Smart Grids
Graduate School of Natural and Applied Sciences
Gazi University
Ankara, Türkiye
ORCID: 0009-0000-8785-1542

Özgün Güngör
Department of Smart Grids
Graduate School of Natural and Applied Sciences
Gazi University
Ankara, Türkiye
ORCID: 0009-0008-9752-4260

Prof. Dr. Erdal Irmak
Department of Electrical&Electronics Engineering
Faculty of Technology
Gazi University
Ankara, Türkiye
ORCID: 0000-0002-4712-6861

Prof. Dr. Erdal Bekiroğlu
Department of Electrical&Electronics Engineering
Faculty of Technology
Gazi University
Ankara, Türkiye
ORCID: 0000-0002-1821-0722

***Abstract*—As small modular reactors (SMRs) take on active roles in smart grid operation, they are expected to provide ancillary services such as primary frequency response, automatic generation control (AGC), and voltage support. Delivering these services demands a communication infrastructure different from that of classical nuclear plant telemetry. This paper examines, at the protocol layer, the grid-side communication architecture connecting SMR facilities to the transmission system operator (TSO; TEİAŞ in Türkiye), using the Turkish power system as the reference context, and proposes a concrete protocol–security mapping for four control layers. First, the timing and interoperability requirements spanning millisecond-to-hourly scales preclude any single protocol from satisfying all four layers. Second, the 3 ms delivery envelope of IEC 61850 GOOSE conflicts with RSA/ECDSA-based signature protection under IEC 62351-6 in software, whereas message authentication code (MAC)-based authentication fits within the same envelope. Accordingly, a layered architecture is proposed that confines GOOSE traffic to an electrically isolated plant zone while employing TLS-secured IEC 60870-5-104 at the grid interface. The proposed architecture is consistent with TEİAŞ's existing infrastructure and Türkiye's 2050 nuclear targets, and its per-layer timing margins are validated by an ns-3 network simulation under realistic packet contention and cross-traffic.**

Keywords*—Smart grid, small modular reactor, IEC 61850, IEC 62351, IEC 60870-5-104, AGC, cybersecurity, latency budget, Turkish power system.

I. Introduction

Conventional nuclear plants run at fixed capacity, and their communication with the transmission system operator (TSO; TEİAŞ in Türkiye) is largely basic SCADA (supervisory control and data acquisition) telemetry. As variable renewables grow, this paradigm becomes insufficient: frequency excursions widen, classical spinning reserves diminish, and more agile control is expected from every grid-connected resource.

SMRs provide a practical solution to this challenge (Fig. 1). With typical capacities up to 300 MWe per module, multi-unit deployment, and load-following capability [1], they are a serious candidate for ancillary service markets. Moreover, an SMR's turbine-generator can operate as a synchronous condenser, providing inertia and short-circuit capacity; Nøland et al. [2] show that in a 100% renewable system, meeting these system-bearing services with synchronous condensers costs approximately 20 USD/MWh system-wide, whereas SMRs can provide the same services in-plant at lower cost.

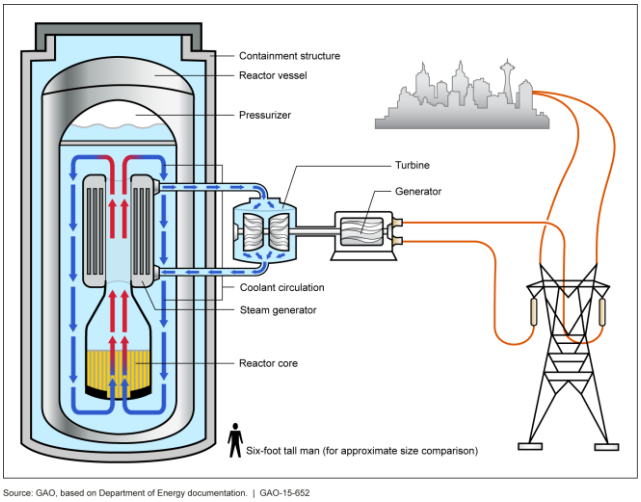

Fig. 1. Illustration of a light water small modular nuclear reactor (SMR). Adapted from [3].

The contributions of this paper are as follows: (i) a concrete protocol mapping for four control layers that jointly accounts for timing, legacy infrastructure compatibility, and security (Table I, Fig. 3); (ii) quantification of the conflict between GOOSE's 3 ms delivery envelope and IEC 62351-6 signature protection as a function of the cryptographic mechanism, and a resulting security architecture combining isolation with TLS; (iii) a communication pattern for multi-module plants that runs set-point disaggregation at the PCS gateway concurrently with intra-plant GOOSE coordination; (iv) demonstration of the proposal's applicability in the Türkiye/TEİAŞ context; and (v) an ns-3 discrete-event network simulation of the four-layer communication path that, under realistic packet contention and cross-traffic, quantitatively validates the latency margin of every control layer and reproduces the GOOSE/IEC 62351-6 envelope conflict (Table III, Figs. 5 and 6).

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

The analysis draws on the IEC 61850, IEC 60870-5-104, IEC 62351, IEC 62443, and CIM standards and current literature. As no commercial-scale ancillary-service-capable SMR yet operates, hardware-in-the-loop validation is not possible; instead, the analysis is anchored to quantitative bounds from the standards and validated by an ns-3 simulation of the four-layer path (Section VI).

II. Background: SMR as an Active Grid Component

An SMR plant's active grid participation depends on coupling the physical process to the control and communication layers (Fig. 2). Reactor modules deliver power to a common turbine-generator via steam generators; the generated electricity is stepped up to the 400 kV transmission network through a main transformer. Three control levels underlie this physical chain: the reactor control system (RCS) of each module, the plant control system (PCS) coordinating them, and the grid interface connecting the PCS to the outside world. Reactor protection functions (Class 1E) remain in a separate, strictly controlled domain and are outside the scope of this paper.

Two SMR characteristics shape communication design. First, the reactor's thermal response time limits the load-following rate [1], so the AGC-loop bottleneck is reactor dynamics, not communication. Second, multi-unit deployment adds a coordination burden absent in single-reactor plants (Section V-C); for the dynamic stability of grid-connected SMRs, see [4].

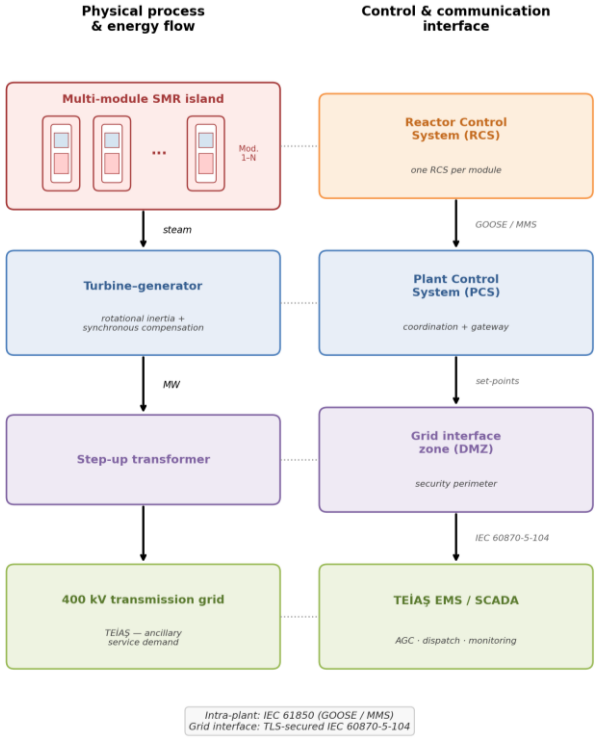

Fig. 2. Mapping of the physical process (left) and the corresponding control/communication interface (right) in a multi-module SMR plant.

III. Proposed Communication Architecture

A. Four-Layer Control Hierarchy

Frequency and dispatch control operates in four tiers acting at different time scales. The tolerable delay at each tier is set by the electromechanical dynamics of the function it performs.

- *Primary frequency control* — sub-second to 30 s; local governor response.
- *Secondary control / AGC* — seconds to minutes; centralized dispatch from the TSO's energy management system (EMS).
- *Tertiary control / economic dispatch* — 15 min to hours; EMS-level optimization.
- *Supervisory SCADA* — continuous; telemetry, alarms, and status monitoring.

B. Protocol-to-Layer Mapping

The proposed mapping is listed in Table I and summarized in Fig. 3. Beyond timing, it accounts for TEİAŞ's existing protocol base, standard maturity, and operational risk, since selecting protocols on latency alone ignores field integration challenges.

TABLE I. Protocol–Layer Mapping

Control Layer	Time Scale	Recommended Protocol	Rationale
Primary frequency	< 500 ms	IEC 61850 GOOSE	Sub-3 ms peer-to-peer latency over Ethernet L2; no TCP overhead
Secondary (AGC)	2–4 s	IEC 60870-5-104	Proven interoperability with TEİAŞ EMS infrastructure
Tertiary (EMS)	5–60 min	CIM (IEC 61968/70)	Semantic data model; priority is data integrity
Supervisory (SCADA)	1–10 s	IEC 60870-5-104 / MMS	Legacy infrastructure compatibility; continuous telemetry



Fig. 3. Mapping of the four control layers to their respective time scale, recommended protocol, and security zone.

C. Time Synchronization

Time synchronization is another critical component. Coordinating intelligent electronic devices (IEDs) and aligning measurements to the same event require synchronization within and across substations [5]. The

required accuracy is application-dependent [5]: ±1 µs for phasor measurement unit (PMU)-based wide-area measurements; 100 µs–1 ms for protection and fast-transient timestamping; and 10 ms or better for AGC and SCADA. GPS-backed PTPv2 (IEEE 1588) satisfies most of these under one framework.

IV. Latency Budget Analysis

A. Primary Frequency Control Layer

This layer has the tightest timing constraint, so its budget is decomposed below. The end-to-end latency is the sum of four components: frequency measurement, 20–40 ms [6], [7]; local signal propagation, 1–5 ms [8], [9]; governor response, 50–200 ms [7]; and turbine-generator response, 200–500 ms (drawn from large-scale pressurized water reactor (PWR) data; SMR-specific validation is required) [7]. The total budget is roughly 271–745 ms, of which communication is under 10 ms (about 1–4%). The limiting factor for primary frequency response is therefore the electromechanical dynamics, not communication latency. GOOSE has wide margin here; the rationale for its 3 ms envelope is cybersecurity, not timing (Section V).

B. Secondary Frequency Control (AGC) Layer

The AGC layer operates with a 2–4 s dispatch cycle, and the dominant bottleneck is the reactor's thermal response time [6], [1]. The 100 ms – 2 s latency achievable with TLS over IEC 60870-5-104 is more than sufficient for this cycle; for this layer, security and interoperability dictate the protocol choice rather than latency.

C. Tertiary / EMS and SCADA Layers

At the EMS layer (5–60 min scan intervals), what matters is data integrity and semantic interoperability rather than low latency, so CIM-based XML exchange within the IEC 61968/61970 framework is appropriate. At the SCADA layer, IEC 60870-5-104 and MMS (Manufacturing Message Specification) are equally suitable for continuous telemetry; for IEC 61850-based frequency regulation, see [10]. Table II compares the four protocols' timing and security.

TABLE II. Protocol Timing and Security Comparison

Protocol	Typical Latency	Transport	Native Security	IEC 62351 Profile
IEC 61850 GOOSE	< 3 ms	Ethernet L2	None	IEC 62351-6
IEC 61850 MMS	50–500 ms	TCP/IP	None	IEC 62351-4
IEC 60870-5-104	100 ms – 2 s	TCP/IP	None	IEC 62351-3, -5
CIM (IEC 61968/70)	Minutes	HTTPS/XMPP	TLS	IEC 62351-8

V. Cybersecurity Constraints

A. IEC 62443 Zone Architecture

An SMR plant providing active grid services is divided into four zones under IEC 62443: reactor protection (Class 1E; out of scope), plant control, grid interface, and corporate. A broad taxonomy of cybersecurity control schemes for smart grids is given in [11]. The most critical point is the channel linking the plant control zone to the grid interface and carrying AGC set-points. The practical consequence of compromising this channel is severe: erroneous dispatch commands could significantly disrupt grid frequency. This threat model typically mandates the application of IEC 62443 Security Level 3–4 to the interface [12], [13]. The zones and the inter-zone flows are depicted in Fig. 4.

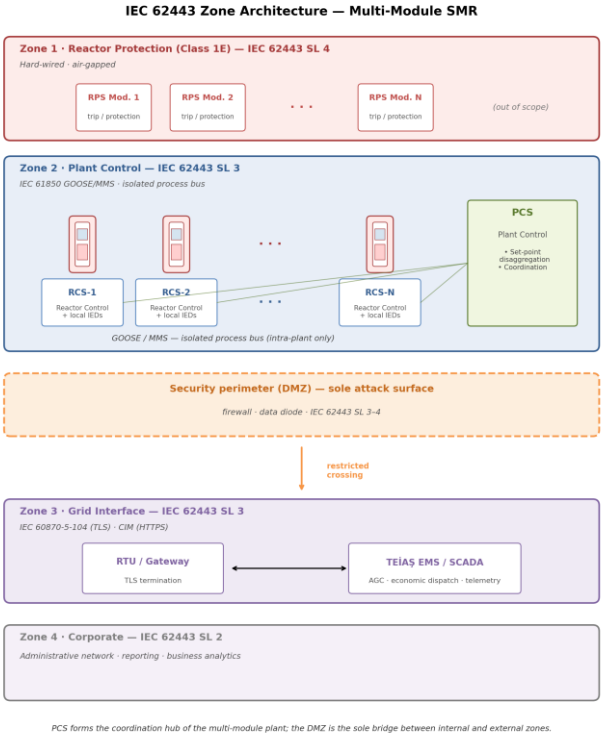

Fig. 4. IEC 62443 zone architecture for a multi-module SMR plant. Each module retains its own reactor protection system (RPS, Class 1E) and RCS, communicating externally only through the PCS via a demilitarized zone (DMZ).

B. Core Design Tension: GOOSE Latency vs. IEC 62351-6

GOOSE messages are subject to a tight 3 ms delivery constraint for communication reliability; the digital signatures prescribed by IEC 62351-6 impose a per-message processing overhead. Hussain et al. [9] demonstrate that RSA- and ECDSA-based signatures exceed this 3 ms envelope on typical IED hardware, rendering them impractical for GOOSE/SV (sampled values) messages; the same work reports that the message authentication code (MAC)-based algorithms recommended in IEC 62351-6:2020 (HMAC-SHA256, AES-GMAC) keep the end-to-end latency below 3 ms. This conflict primarily arises during implementation rather than in theory.

Hardware acceleration (e.g., an FPGA) can also keep RSA/ECDSA within 3 ms [8], but on general-purpose IED hardware the same mechanism frequently exceeds the envelope [9]. Although MAC-based authentication resolves the constraint in software, an extra protection layer is still preferred to minimize the attack surface. The proposed architecture therefore confines GOOSE traffic to an electrically isolated plant control zone and runs grid-interface communication over IEC 60870-5-104 secured with TLS (IEC 62351-3), whose overhead is manageable [14].

Herath et al. [15] measure IEC 62351-compliant MAC authentication at 0.38 ms average / 0.64 ms maximum, and a MAC-plus-semantic-IDS hybrid at 0.54 ms / 0.88 ms—both well within the 3 ms Type 1A requirement. These figures

come from modest hardware without optimization; validation on SMR-class IED hardware remains open.

C. Architecture for Multi-Module SMR Plants

Plants housing 4–12 reactor modules pose challenges not seen in large conventional plants. Each module has its own RCS, but all communicate externally through a shared PCS gateway. Communication is organized in three flows: (i) inter-module coordination (e.g., a joint frequency response) via GOOSE within the isolated plant network; (ii) module-specific set-points from the TSO, disaggregated at the PCS gateway and distributed to the relevant RCS instances via MMS; and (iii) the PCS gateway itself, which forms the security perimeter and is the sole attack surface. Isolation and hierarchy thus keep the simultaneous coordination of multiple RCS instances manageable.

VI. Performance Evaluation by ns-3 Network Simulation

As no commercial-scale ancillary-service-capable SMR yet operates, hardware-in-the-loop testing on a real plant is not possible. We therefore implemented the architecture as an executable model in the ns-3 discrete-event simulator (v3.44) and measured end-to-end latency under realistic packet contention, switch forwarding, and wide-area queueing. Unlike a closed-form budget, the simulator reproduces medium-access contention and cross-traffic jitter, so the figures emerge from simulated packet flows rather than the analytical bounds of Section IV.

A. Simulation Model and Parameters

The architecture is modeled as two coupled segments. The isolated plant zone is a switched 100 Mbps Ethernet L2 segment in which N reactor-module IEDs (N = 4, 8, 12) and the PCS gateway each attach through a dedicated link to an explicit store-and-forward bridge (ns-3 BridgeNetDevice), so that every host occupies its own collision domain as in a real substation switch. Each IED emits 200-byte GOOSE-class APDUs at a fixed 2 ms publish cadence with staggered start times, so frames genuinely contend for the switch egress port. The transport is modeled as an application-layer UDP datagram flow used as a tractable proxy for GOOSE/104 framing: it faithfully reproduces medium access, switch forwarding, propagation, and queueing, but does not implement the IEC 61850 L2 multicast stack or the exponential GOOSE retransmission profile, and the publish cadence is held fixed rather than event-triggered. The grid interface is a two-hop wide-area link (PCS gateway → edge router → TSO EMS) carrying IEC 60870-5-104 set-points on a 2 s AGC cycle, with competing SCADA cross-traffic generated by a bursty On/Off source to induce queueing and jitter. Wire-level latency (medium access, switch forwarding, propagation, queueing) is measured directly by the ns-3 FlowMonitor. To this we add the host-side IEC 62351 processing cost that the network layer does not capture and that is not a network-derived quantity: per-message MAC signing/verification of 0.38 ms (HMAC-SHA256/AES-GMAC, after Herath et al. [15]), the MAC-plus-semantic-IDS hybrid at 0.54 ms [15], and software RSA/ECDSA signing of approximately 5 ms drawn from the multi-millisecond range reported by Hussain et al. [9]; the grid link additionally bears 80–400 ms of amortized TLS and IEC 60870-5-104 stack processing [14]. Because the crypto cost is injected rather than simulated, the RSA/ECDSA deadline outcome follows deterministically from this per-message cost; the simulation's role is to quantify the network margin and show how much of the 3 ms budget remains for the cryptographic layer. Each scenario is run over eight independent random seeds: every GOOSE scenario yields on the order of 10^3–10^4 delivered frames and the AGC scenario 400 dispatch messages. Reported means are accompanied by their across-seed standard deviation, and the 95% confidence interval of the mean is below 0.02 ms for the GOOSE scenarios and below 7 ms for AGC, so the per-layer margins below are stable across seeds rather than artifacts of a single run.

B. Results

Table III reports the ns-3 outcome for each layer; Fig. 5 shows the GOOSE delivery distribution and Fig. 6 its scaling with module count. In the isolated plant zone, GOOSE secured with MAC is delivered in 0.70 ms on average (standard deviation 0.19 ms across seeds; 99th percentile 1.12 ms) for a 12-module plant, with zero frames exceeding the 3 ms Type 1A envelope. Crucially, this margin is essentially flat across plant size — mean latency moves only from 0.65 ms at four modules to 0.70 ms at twelve (Fig. 6) — confirming that the switched plant zone absorbs multi-module contention without eroding the timing budget; because each host occupies its own collision domain, adding modules adds egress-port load at the gateway rather than shared-medium contention. The near-constant 99th percentile across module counts reflects that, at these light frame rates, tail latency is governed by the fixed publish cadence and switch forwarding rather than by congestion. The MAC-plus-IDS hybrid stays at 0.86 ms mean / 1.30 ms p99, also entirely below the envelope. By contrast, the injected software RSA/ECDSA cost pushes essentially every frame above 3 ms (mean 5.29 ms, p99 7.10 ms, 99.9% deadline miss); since the per-message signing cost alone (≈5 ms) exceeds the budget, this outcome follows from the cryptographic mechanism rather than from network contention and quantifies why software RSA/ECDSA is rejected for GOOSE. On the grid interface, AGC set-points over TLS-secured IEC 60870-5-104 are delivered in 241 ms on average (standard deviation 65 ms across seeds; p99 395 ms) even under competing SCADA cross-traffic, never approaching the 2 s dispatch cycle.

TABLE III. NS-3 NETWORK SIMULATION RESULTS (12-MODULE PLANT UNLESS NOTED)

Scenario	Mean	99th pct.	Deadline miss
GOOSE + MAC, 4 modules	0.65 ms	1.08 ms	0.00%
GOOSE + MAC, 8 modules	0.67 ms	1.10 ms	0.00%
GOOSE + MAC, 12 modules	0.70 ms	1.12 ms	0.00%
GOOSE + MAC + IDS, 12 modules	0.86 ms	1.30 ms	0.00%
GOOSE + RSA/ECDSA SW, 12 modules	5.29 ms	7.10 ms	99.9%
AGC over TLS-104 (vs 2 s)	241 ms	395 ms	0.00%

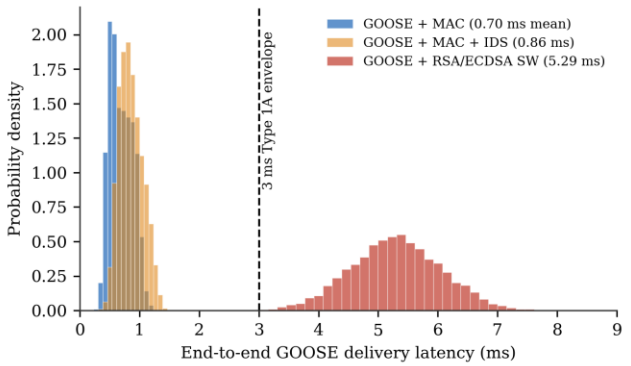

Fig. 5. ns-3 distribution of end-to-end GOOSE delivery latency for a 12-module plant under three protection mechanisms, relative to the 3 ms Type 1A envelope (dashed line).

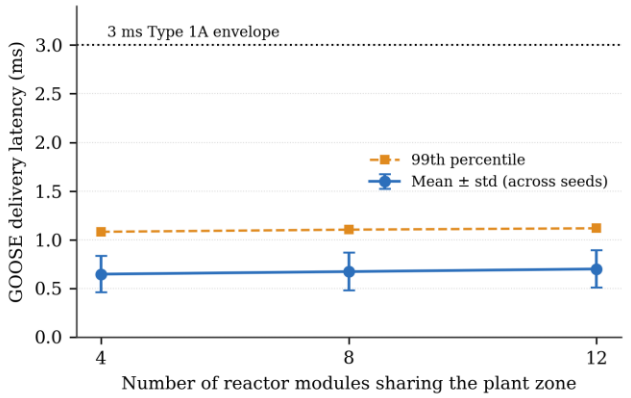

Fig. 6. Simulated GOOSE delivery latency (MAC) versus the number of reactor modules sharing the isolated plant zone.

These results corroborate the decisions of Sections III–V with an executable network model and isolate the network contribution that Section IV could only estimate. The model abstracts the host in two ways: the GOOSE/104 framing is represented by a UDP datagram proxy rather than the full IEC 61850 multicast stack, and the crypto and TLS costs are injected from published measurements rather than measured on SMR-class IED hardware; reactor dynamics also lie outside the model. It is therefore an architecture-level feasibility result that complements, but does not replace, the hardware measurements identified as future work.

VII. Turkish Power System Context

TEİAŞ operates the 400 kV transmission network with approximately 125 GW of installed capacity [16]. In the current mix, renewables account for approximately 62% of the total capacity, natural gas for 20%, and coal for 18%; the nuclear share is currently zero. Observer membership in ENTSO-E (the European Network of Transmission System Operators for Electricity) since January 2023 institutionally supports the alignment of national grid operation standards with continental European norms.

Two milestones are pivotal in Türkiye's long-term planning (Fig. 7): by 2035, scaling wind and solar to 120 GW and nuclear capacity to 7.2 GW; and, in line with the 2053 net-zero target, reaching 20 GW of nuclear by 2050, with 5 GW of that earmarked for SMRs — one quarter of the 2050 nuclear portfolio [17], [18]. For the legal framework and the policy process, the reader is referred to [19].

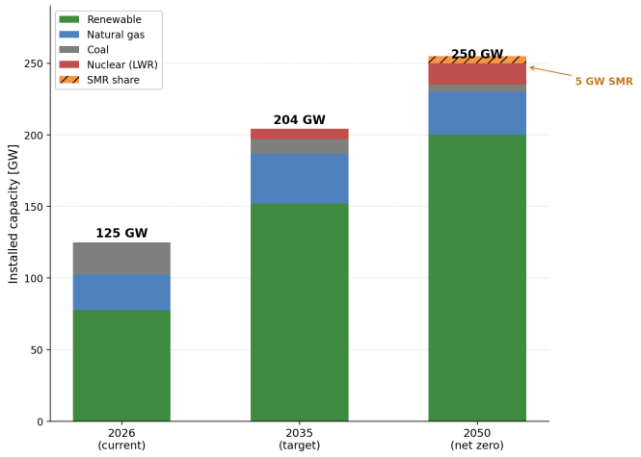

Fig. 7. Turkish power system installed-capacity targets — 2026 (current), 2035, and 2050.

Based on publicly available data, TEİAŞ's supervisory infrastructure relies predominantly on IEC 60870-5-104-based RTU (remote terminal unit) connectivity; IEC 61850 adoption appears only in new substation projects to date. As plant-level protocol inventories are not publicly disclosed, this is an observational finding. The practical implication is that implementing the proposed architecture requires no radical infrastructure overhaul on the TEİAŞ side. IEC 60870-5-104 with the IEC 62351-3 profile at the grid interface is directly compatible with existing systems, while the in-plant IEC 61850 architecture aligns with the international best practice exemplified by the Shin-Kori 3-4 experience [20], [21].

VIII. Conclusion

This paper examined, at the protocol layer, the grid-side communication architecture required for SMRs to take an active role in the smart grid and presented a concrete proposal in the Turkish context. First, no single protocol can satisfy all layers; the layered mapping—GOOSE for primary frequency, IEC 60870-5-104 for AGC and SCADA, and CIM for EMS (Table I)—jointly meets the timing and operational criteria. Second, the tension between GOOSE's 3 ms envelope and IEC 62351-6 protection depends on the cryptographic choice. RSA/ECDSA exceeds the envelope on typical IEDs [9], MAC-based algorithms fit within it even in software [15], [9], and hardware acceleration widens the margin [8]. GOOSE is therefore confined to an isolated plant zone, and TLS-secured IEC 60870-5-104 is used at the interface. Third, multi-module plants require set-point disaggregation at the PCS gateway to run concurrently with intra-plant GOOSE coordination. Fourth, the proposal is consistent with TEİAŞ's existing infrastructure and 2050 targets. Fifth, an executable ns-3 model of the four-layer path independently confirms these claims under realistic switch forwarding, queueing, and cross-traffic. GOOSE secured with MAC is delivered within 1.12 ms (99th percentile) and stays flat as the plant scales to twelve modules. AGC over TLS-104 never approaches its 2 s cycle even under cross-traffic, and the rejected software RSA/ECDSA configuration breaches the 3 ms GOOSE envelope once its injected per-message signing cost is accounted for.

The principal limitation of the study is that hardware-in-the-loop experimental validation on a real SMR is not yet

possible at this stage: the turbine-generator parameters are drawn from large-scale PWR experience [7], [1], and the IEC 62351-6 latency data from general-purpose laboratory environments [15]. The ns-3 network simulation in Section VI mitigates this gap by confirming the per-layer timing margins under realistic contention, but its host-side crypto and TLS costs are still injected from published laboratory measurements rather than measured on SMR-class hardware. Future work should focus in three directions: (i) measuring IEC 62351-6 processing latencies on SMR-class IED hardware; (ii) validating the multi-module pattern against commercial SMR control interfaces; and (iii) calibrating the latency budgets with SMR-specific thermal and electromechanical data.

REFERENCES

[1] Z. Zhang and J. Jiang, "On Load-Following Operations of Small Modular Reactors," Prog. Nucl. Energy, vol. 173, art. no. 105274, 2024.

[2] J. K. Nøland, M. Hjelmeland, M. Korpås, and L. B. Tjernberg, "The Potential of Small Modular Reactors to Provide System-Bearing Services in the Future Power Grid," in Proc. IEEE PES ISGT-Europe, Dubrovnik, Oct. 2024, pp. 1–6.

[3] U.S. Government Accountability Office, “Technology Assessment: Nuclear Reactors—Status and Challenges in Development and Deployment of New Commercial Concepts,” GAO-15-652, Washington, D.C., Jul. 2015. [Online]. Available: https://www.gao.gov/products/gao-15-652

[4] S. Badakhshan, R. A. Jacob, A. Mahboub Rad, C. Pan, Y. Li, and J. Zhang, “Dynamic Stability Assessment of Grid-Connected Data Centers Powered by Small Modular Reactors,” arXiv:2603.09110, Mar. 2026. [Online]. Available: https://arxiv.org/abs/2603.09110

[5] D. Macii and S. Rinaldi, "Time Synchronization for Smart Grids Applications: Requirements and Uncertainty Issues," IEEE Instrum. Meas. Mag., vol. 25, no. 6, pp. 11–20, Sep. 2022.

[6] ENTSO-E, *Continental Europe System Protection Plan—Load-Frequency Control Requirements*, Brussels, 2019.

[7] P. Kundur, Power System Stability and Control. New York: McGraw-Hill, 1993.

[8] M. Rodríguez, J. Lázaro, U. Bidarte, J. Jiménez, and A. Astarloa, "A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems," IEEE Access, vol. 9, pp. 51646–51657, 2021.

[9] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

[10] L. Tightiz, H. Yang, and H. Bevrani, "An Interoperable Communication Framework for Grid Frequency Regulation Support from Microgrids," Sensors, vol. 21, art. no. 4555, 2021.

[11] A. Insfrán and B. Barán, "Taxonomy and survey on cybersecurity control schemes for smart grids," IET Smart Grid, 2025.

[12] OECD Nuclear Energy Agency, "Consensus Position on the Impact of Cyber Security Features on Digital I&C Systems Important to Safety at Nuclear Power Plants [CP-08]," NEA/CNRA/R(2021)2, OECD Publishing, Paris, Nov. 2022.

[13] IEC SC45A, "The IEC Standard Series on Cybersecurity for I&C and Electrical Systems for Nuclear Power Plants and SMRs," presented at the IAEA Int. Conf. SMRs, Vienna, Oct. 2024, paper no. 292.

[14] M. G. Todeschini and G. Dondossola, "Securing IEC 60870-5-104 Communications Following IEC 62351 Standard: Lab Tests and Results," in Proc. AEIT Int. Annu. Conf., 2020, pp. 1–6.

[15] A. Herath, C. C. Liu, J. Hong, and K. Park, "Evaluation of Real-Time Mitigation Techniques for Cyber Security in IEC 61850 / IEC 62351 Substations," in Proc. CIGRE US Nat. Comm. Grid of the Future Symp., 2025.

[16] Türkiye Elektrik İletim A.Ş. (TEİAŞ), "General Daily Operation Result," May 2, 2026. [Online]. Available: https://www.teias.gov.tr. Accessed: Jun. 9, 2026.

[17] Republic of Turkey Ministry of Energy and Natural Resources, Turkey National Energy Plan: 2035 and 2050 Targets, 2025.

[18] Republic of Turkey Ministry of Energy and Natural Resources, "Minister Bayraktar Announced Turkey's 2050 Target at ISO," Nov. 26, 2025. [Online]. Available: https://enerji.gov.tr. Accessed: Jun. 9, 2026.

[19] O. C. Artantaş, "Turkey's Nuclear Energy Aspirations: Policy Challenges and Legal Trajectory," J. World Energy Law & Bus., vol. 17, no. 3, pp. 201–214, 2024.

[20] C.-K. Chang, "IEC 61850 based electrical protection and control system for nuclear power plants," J. Nucl. Energy Sci. Power Generat. Technol., vol. 8, no. 2, 2019.

[21] S. Kumar, A. Abu-Siada, N. Das, and S. Islam, "Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System," Electronics, vol. 12, no. 15, art. no. 3345, 2023.