Closing the Hosting Capacity Data Frequency Gap

Written input to the DESAP D4.1 roadmap

Sent to the ENTSO-E JTF, 2 April 2026

Abhishek Arya, AlfaTouro Consulting

SUBMISSION BY EMAIL TO THE JTF MEMBERS OF ENTSO-E To: uros.salobir@entsoe.eu; flore.patrat-delon@eudsoentity.eu CC: siddhesh.gandhi@entsoe.eu; omar.huarcaya@eudsoentity.eu; franck.diawagoum@entsoe.eu Subject: Written Input to DESAP D4.1 Roadmap — Hosting Capacity Data Frequency Gap — Abhishek Arya MAIL BODY SENT - Dear Mr. Salobir and Ms. Patrat-Delon, Please find attached a written input to the DESAP D4.1 roadmap process, submitted following my attendance at the Digital Twins seminar on 2 April 2026, where I raised the question of hosting capacity map update frequency in the context of federated digital twin architecture. The input identifies the gap between the annual Article 31 publication cycle and the real-time data dependency of UC2.1 and UC3, proposes a resolution architecture requiring no new communication infrastructure beyond a substation RTU upgrade and protocol specification, addresses the cybersecurity implications at the federation interface, and names three specific regulatory instruments through which the gap can be closed — all grounded in a five-paper EU grid architecture research series published on Zenodo and SSRN in 2026. I am available to participate in Advisory Board stakeholder engagement activities or in D4.1 cluster calls relevant to the technical architecture or regulatory instrument workstreams. Yours sincerely, Abhishek Arya Independent Infrastructure Strategist THE ATTACHMENT WITH RECOMMENDATION AS FOLLOWS: Closing the Hosting Capacity Data Frequency Gap in Federated Digital Twin Architecture. Submitted by: Abhishek Arya Category: Research Institution / Academia Date: April 2026 Addressed to: Joint Task Force DESAP Co-Chairs, ENTSO-E and DSO Entity Prior engagement: TYNDP 2026 System Needs Consultation (March 2026); DESAP Digital Twins Seminar (2 April 2026) 1. Purpose of this Input The DESAP initiative has produced a well-structured, technically rigorous framework for Digital Twin Development across Europe’s electricity system. The D3.1 report, published January, 2026, successfully translated strategic ambitions into four implementable use cases: consumer-centric flexibility (UC1), enhanced network planning (UC2.1), HILF resilience (UC2.2), and coordinated TSO_DSO security assessment (UC3). The collaborative design methodology, two rounds of dedicated cluster calls, expert feedback, and IEC 62559 use case definition, reflects genuine progress in aligning a complex, multi-stakeholder architecture. This input is submitted in that constructive spirit. It identifies one structural precondition that the D4.1 roadmap will need to address in Phase 1 (Minimum Viable Solution) before UC2.1 and UC3 can function as their architecture intends. The precondition exists not because of a gap in the technical design, which is sound, but because it sits at the intersection of two separate regulatory regimes that no single workstream currently owns: the EU Electricity Directive’s hosting capacity publication requirement and the NIS2 Directive’s compliance framework for distributed energy entities. This input names that intersection precisely and proposes a resolution pathway that requires no new large-scale communication infrastructure, drawing on the EU Grid Architecture Research Series published on Zenodo and SSRN in 2026.

2. The Precondition: Hosting Capacity Data Frequency 2.1. The Architecture’s Data Dependency The federated digital twin architecture assumes that DSO twins expose current hosting capacity data to the TSO layer and to the federation interface. UC2.1 (enhanced network planning) depends on TSOs accessing distribution-layer capacity constraints to coordinate investment decisions. UC3 (coordinated security assessment) depends on a shared, synchronised view of transmission and distribution grid state across all voltage levels. Both use cases, as designed, require that the DSO-layer data reflect actual current network conditions at the point of ingestion by the federation. 2.2. The Regulatory Reality DSO hosting capacity maps are currently published annually under Article 31 of the EU Electricity Directive (2019/944). These maps are static, scenario-based power flow analysis outputs, aggregated to

feeder or substation level, modelling peak load and peak generation as separate scenarios rather than combined operational states. They are not updated dynamically, and they are not formally cross-referenced into TSO planning frameworks. In fast-electrifying metropolitan networks, where EV penetration, heat pump adoption, and data centre baseload are growing simultaneously, a hosting capacity map published in January may not accurately reflect the network's operational envelope by October. The structural dynamics behind this drift are documented in The Urban Blind Spot: Aligning Electrification Ambition with Distribution Reality (SSRN: 10.2139/ssrn.6309321; Zenodo: 10.5281/zenodo.18999988) and Sequencing Electrification Under Distribution Congestion (SSRN: 10.2139/ssrn.6349618; Zenodo: 10.5281/zenodo.19000382), which document the transmission–distribution interface visibility gap from a planning methodology perspective. 2.3. The Consequence for D4.1 Phase 1 The federated digital twin is designed to make the TSO–DSO interface operationally transparent in a way that static, annually published maps cannot. For UC2.1 and UC3 to deliver on this design intent, the data pipeline feeding the DSO twin must be capable of reflecting the current network state. Where that pipeline depends on Article 31 maps in their present form, the gap between data vintage and operational reality will persist inside the digital twin architecture, regardless of the quality of the federation layer itself. The D4.1 roadmap should classify this as a red-category Phase 1 precondition, using the roadmap's own traffic-light priority framework, because it conditions the functional performance of use cases already defined in D3.1. It is most efficiently addressed at the inception of the implementation phase, before platform and interface investments are committed around a data pipeline that remains annual in cadence. 3. The Resolution Architecture: Dynamic Hosting Capacity as a Byproduct The resolution does not require a new parallel monitoring infrastructure programme. It requires standardising a communication architecture that must be built in any case for distributed energy resource grid integration, and specifying that this architecture produces dynamic hosting capacity data as a structural byproduct of connections that already need to exist. 3.1. Architecture Description The architecture operates across four levels: Asset to substation: CPO-aggregators, managing BESS, solar, and EV charging clusters as unified grid assets, connect to their host secondary substation via a dedicated local link specified as IEC 61850 GOOSE over a copper pair or fibre run alongside the power connection at commissioning. This avoids the PLC noise interference introduced by grid-forming inverters and uses a hardened, deterministic protocol already within the IEC 61850 framework. Substation aggregation: The secondary substation aggregates asset-level operational data, BESS state of charge, charger load, solar generation output, and transformer thermal status, and computes, locally, the real-time utilisation state of that transformer. This produces a continuously updated snapshot of available headroom at that node.** Substation to DSO: The aggregated summary is transmitted to the DSO central server through the substation's existing hardened backhaul channel, which already carries transformer telemetry. No new backhaul infrastructure is required. The DSO server aggregates across substations into a continuously updated hosting capacity dataset. DSO to TSO (one-way): A structured hosting capacity signal is transmitted to the TSO twin via a one-way data architecture, functionally a data diode. The TSO consumes this signal for planning and coordination purposes. No return command channel exists, which is both sufficient for the TSO's planning needs and architecturally correct from a security standpoint. 3.2. Deployment Dependency and Progressive Scalability One clarification is important for D4.1 scoping purposes. The architecture described above uses the CPO-aggregator node as its reference deployment vehicle because it represents the most data-rich connection type, integrating BESS, solar, and EV charging load in a single metered asset. However, the substation aggregation function does not depend exclusively on CPO-aggregator deployments. Any DER connection carrying a monitored load or generation profile, EV chargers, heat pumps, rooftop solar inverters, and standalone BESS, generate the same class of transformer utilisation data when connected via a specified local protocol to the substation RTU. The data pipeline, therefore, scales progressively with DER deployment density rather than depending on a specific asset threshold being reached first. This has a direct implication for D4.1 Phase 1 scoping: the critical deliverable at the MVS stage is not deployment, but protocol, specification,

standardising the local link requirements and minimum data set for any new DER connection to a secondary substation. Each connection made under that specification adds a data point to the hosting capacity dataset. Coverage improves continuously as deployment proceeds, rather than materialising only after a deployment threshold is crossed. The architecture is viable at day one of the first connection, and improves with every subsequent one. 3.3. Properties relevant to D4.1 This architecture has three properties the roadmap should record: Infrastructure reuse: The substation backhaul is in place. The power connection for CPO-aggregator assets must be made regardless of digital twin requirements. The only additional capital cost is an RTU upgrade at the secondary substation to handle the additional data aggregation function, and protocol standardisation between the CPO-aggregator and substation at commissioning. This is materially less expensive than a standalone distribution monitoring rollout. Continuous data generation: Dynamic hosting capacity data is produced continuously as a structural output of normal asset operation, not collected by a separate monitoring programme. This converts an expensive data acquisition challenge into a connection specification. Fail-safe local control: If the substation loses its backhaul connection to the DSO central server, the ANM controller defaults to a conservative local operating mode, curtailing flexible connections to a defined safe percentage until connectivity is restored. This preserves distribution network integrity independent of the broader federation. The full commercial and regulatory architecture underpinning this deployment model is developed in Charging Without Subsidy: How the CPO-Aggregator Framework Unlocks Community-Scale Distributed Energy Investment in Europe (SSRN: 10.2139/ssrn.6468098; Zenodo: 10.5281/zenodo.19219693) and the cybersecurity compliance framework in Securing the Node (SSRN: 10.2139/ssrn.6494558; Zenodo: 10.5281/zenodo.19331391), which together establish the CPO-aggregator community node as the deployment vehicle for this data architecture. The D4.1 roadmap should include, as a Phase 1 (MVS) specification task, the protocol standard for CPO-aggregator to secondary substation communication and the minimum data set required for dynamic hosting capacity computation at the substation level. 4. The Cybersecurity Dimension The DESAP D3.1 report correctly identifies cybersecurity as a key enabler across all four use cases and references IEC 62443 as a relevant standard. This section supplements that framing with a specific vulnerability class introduced by the federation itself, and a concrete validation mechanism that addresses it. 4.1. The Federation Attack Surface A federated digital twin architecture creates a class of vulnerability that is absent in isolated twins: a compromised DSO twin can inject false hosting capacity data into the TSO twin, causing the TSO to make operational decisions, redispatch, investment, contingency response, based on a distribution-layer state that does not exist. At the deployment scale, coordinated false data injection across multiple DSO twins constitutes a systemic risk to TSO operational integrity, not merely a local data quality issue. The scale of this risk at community node deployment levels is quantified in Securing the Node (Zenodo: 10.5281/zenodo.19331391), using TenneT's published FCR obligation figures as the baseline. The analysis demonstrates that coordinated manipulation of a relatively small number of distributed energy nodes is sufficient to create grid-level consequences, making the integrity of the DSO-to-TSO data channel a national security question, not merely an operational one. 4.2. Physics-Based Validation at the Federation Interface The countermeasure is physics-based validation at the federation interface: incoming hosting capacity data from a DSO twin is validated against the physical feasibility constraints of the substations it represents before ingestion into the TSO twin. A reported hosting capacity inconsistent with the thermal limits of the relevant transformer stack is flagged and rejected before it propagates to the TSO planning layer. This framework, developed in Securing the Node for FCR dispatch signal validation, maps directly onto the federation interface requirement. It does not require withholding data from the federation; it requires checking incoming data against independently verifiable physical constraints before accepting it. Implementation is achievable within the IEC 62443 framework already referenced in D3.1, and can be specified as a minimum standard for DSO–TSO data exchange at the federation layer. 4.3. The NIS2 Compliance Gap A secondary gap warrants inclusion in the D4.1 roadmap. NIS2 Directive Article 21 does not currently define a compliance pathway for CPO-aggregator entities, the distributed energy

nodes that are the primary source of the dynamic hosting capacity data proposed in Section 3. If community-scale DER nodes cannot achieve NIS2 compliance, the data they produce cannot be certified for ingestion into critical infrastructure digital twins, and the architecture in Section 3 cannot be formally deployed. This compliance gap is mapped in full, with responsible actors, legislative vehicles, and precedents, in Securing the Node. The resolution requires ENISA to develop Article 21 implementation guidelines that define a compliance pathway for multi-investor shared infrastructure nodes. The architecture proposed in Section 3 and the NIS2 compliance requirement in this section are, ultimately, the same regulatory drafting task. The D4.1 roadmap should include NIS2 compliance pathway definition for CPO-aggregator entities as a Phase 1 prerequisite for the data pipeline described in Section 3, and should specify physics-based federation interface validation as a minimum cybersecurity standard for DSO–TSO data exchange. 5. Regulatory Instruments Required Three instruments, taken together, are sufficient to close the gap identified in this input. Each carries a named responsible actor, a named legislative vehicle, and an existing precedent. Instrument 1 - Article 31, EU Electricity Directive (2019/944) Actor: European Commission / Member State transposition authorities Vehicle: Amendment to Article 31 mandating dynamic hosting capacity publication for DSOs in designated electrification-dense metropolitan areas, with a defined minimum update frequency at MV/LV substation level via a standardised API. Precedent: Denmark's Flexibility.dk platform, which provides near-real-time flexibility capacity data for DSO/aggregator coordination, demonstrating operational viability at the national scale. Rationale: The annual publication cadence established under Article 31 was appropriate for a slowly evolving planning tool. It is not sufficient as the data input for a real-time federated operational system. The amendment should be scoped to electrification-dense zones where the gap between annual publication and operational reality is widest, allowing for phased implementation. Instrument 2 - ACER Network Code on Demand Response (submitted to EC, 7 March 2025) Actor: ACER / European Commission Vehicle: NC-DR framework specification of the standardised data exchange protocol for CPO-aggregator to secondary substation communication, IEC 61850 GOOSE over a dedicated local link, and definition of the minimum data set (transformer utilisation, BESS SoC, charger load, solar output) required for dynamic hosting capacity computation at substation level. Precedent: UK Ofgem RIIO-ED2 framework, specifically Western Power Distribution's Dynamic Network Access deployment enabled by secondary substation monitoring at scale, demonstrating that substation-level real-time data collection is operationally and commercially viable within a regulated network operator framework. Rationale: Converting the architecture in Section 3 from a de facto proposal into a mandated standard deployable across all EU member states requires a network code specification. The NC-DR submission window provides the legislative vehicle. Instrument 3 - ENISA NIS2 Article 21 Implementation Guidelines Actor: ENISA / European Commission Vehicle: ENISA Article 21 implementation guidelines defining a compliance pathway for CPO-aggregator entities and multi-investor shared infrastructure nodes participating in federated digital twin data exchange, and specifying physics-based federation interface validation as a minimum-security standard for DSO/TSO data sharing. Precedent: ENISA's existing NIS2 sectoral guidance for energy operators under Article 21(2), which provides the drafting template for entity-type-specific compliance pathways. Rationale: Without a defined compliance pathway, community-scale DER nodes cannot be formally certified for critical infrastructure data exchange, and the architecture in Section 3 remains legally undeployable regardless of its technical soundness. This is a drafting task, not a research task. 6. Context and Prior Engagement This input is grounded in the EU Grid Architecture Research Series, five papers published on Zenodo and SSRN in 2026, functioning as an integrated implementation stack addressing the transmission-distribution interface visibility gap, distribution congestion sequencing, community-scale distributed energy commercial architecture, and NIS2 cybersecurity compliance: The Urban Blind Spot, SSRN: 10.2139/ssrn.6309321 | Zenodo: 10.5281/zenodo.18999988 Sequencing Electrification Under Distribution Congestion, SSRN: 10.2139/ssrn.6349618 | Zenodo: 10.5281/zenodo.19000382 The Next Grid: Why Ukraine's Reconstruction Is the EU's Most Important Energy Policy Experiment, Zenodo: 10.5281/zenodo.19110430 Charging Without Subsidy, SSRN: 10.2139/ssrn.6468098 | Zenodo:

10.5281/zenodo.19219693 Securing the Node, SSRN: 10.2139/ssrn.6494558 | Zenodo: 10.5281/zenodo.19331391 This input is submitted in connection with a formal written response to the ENTSO-E TYNDP 2026 System Needs Methodology consultation (Arya Infrastructure Strategy, March 2026), and attendance and substantive engagement at the TYNDP 2026 stakeholder webinar (27 March 2026) and the DESAP Digital Twins seminar (2 April 2026), where the hosting capacity update frequency question was raised directly with the panel.