Oren Moreno

ITAI 3377

Professor Patricia McManus

April 28, 2025

Capstone Project: Autonomous Microgrid Optimization System

**1. Project Proposal**

The Autonomous Microgrid Optimization System (AMOS) is designed to revolutionize operational management within campus, industrial park, and remote-community microgrids. AMOS leverages generative AI and real-time edge computing to optimize distributed energy resources (DERs), aiming to maximize renewable energy utilization, reduce operational costs, and enhance system resilience. Through a closed-loop autonomy cycle of Sense, Predict, Plan, Act, and Learn, AMOS minimizes dependence on centralized infrastructure while maintaining stringent security, privacy, and regulatory compliance.

AMOS targets several critical outcomes, including reducing energy wastage by 15-20%, achieving 95% renewable utilization during peak generation, cutting grid imports by 30%, trimming operational expenditures by 25%, and providing a return on investment within 24 months. The system also aims to deliver 99.9% availability with ±3% voltage stability, with additional revenue opportunities from optimized grid trading.

AMOS’ generative AI approach has two main components: it utilizes a lightweight Transformer-based Forecast Generator to synthesize 24-hour scenarios for solar irradiance, wind speed, load, and price forecasting with ≥90% accuracy, and a Model-Predictive Reinforcement Learning agent to generate rolling 15-minute schedules for each DER. The system operates on ARM-based edge accelerators with localized data processing to ensure privacy and latency requirements.

**2. System Architecture (Conceptual)**

AMOS is structured around a robust and resilient Sense → Predict → Plan → Act → Learn autonomy loop, operating across five key conceptual layers that together ensure comprehensive optimization, real-time responsiveness, and high security.

* **DER & Sensor Layer:** Distributed Energy Resources (solar inverters, wind turbine controllers, battery management systems, smart meters, and weather stations) continuously generate telemetry data at 1–5 second intervals. Communication is conducted using industrial protocols such as Modbus-TCP, IEC 61850, and CAN-FD, with AES-GCM encryption applied to secure the data exchanges. Sensors are hardened against firmware tampering via secure boot mechanisms and regular firmware signing.
* **Edge Gateway (IoT Hub):** The Edge Gateway aggregates, normalizes, and validates incoming telemetry streams, ensuring data quality before forwarding to the Edge AI layer. The gateway maintains a 24-hour in-memory database for rapid query and rollback operations. It supports over 10,000 telemetry points per second via MQTT v5 (TLS 1.3) and OPC-UA Pub/Sub protocols, using hardware-based TPM modules for secure key storage.
* **Edge AI Runtime:** Hosting the Forecast Generator and MPC-RL Agent, the Edge AI Runtime executes local predictions and optimizations without cloud dependencies. Data flows into the runtime as feature tensors, processed by rootless containers isolated via SELinux policies. Communication with control interfaces happens through gRPC with protobuf payloads for minimal overhead and maximal security.
* **Control Interface Layer:** This layer ensures near-instantaneous execution of dispatch decisions, communicating setpoints to DER controllers and market interfaces with latencies consistently below 100 milliseconds. It uses IEC 61850-MMS for supervisory control and OpenADR 2.0b for automated market bidding, backed by robust mutual TLS authentication with rotating short-lived SPIFFE certificates and strict RBAC enforcement.
* **Cloud/Fleet Operations Layer (Optional):** Although AMOS prioritizes local operation, a cloud layer facilitates nightly federated learning aggregation, remote firmware updates, and long-term analytics. All cloud interactions are encrypted with HTTPS (TLS 1.3) and employ differential privacy to protect site-level confidentiality. The fleet manager also monitors drift detection signals, initiating retraining when necessary.

Together, these layers enable a zero-trust, self-healing, and self-optimizing microgrid management system that guarantees rapid sense-to-act cycles, privacy preservation, and scalable fleetwide improvements.

**3. AI Model Development (Conceptual)**

AMOS deploys two synergistic generative AI models at the edge to enable predictive forecasting and autonomous dispatch optimization.

The Forecast Generator is an edge-tuned Transformer model utilizing probabilistic cross-attention to generate 24-hour multivariate scenario forecasts. It samples latent spaces using variational techniques and augments extreme events with WGAN-GP modules. Inputs include 72-hour historical telemetry, weather forecasts, and tariff data. The model is optimized post-training for INT8 quantization, achieving cold-start latency under 75 milliseconds.

The MPC-RL Dispatch Agent uses a hybrid approach, combining differentiable physics-informed simulators with PPO-Clip reinforcement learning. It refines actions through cross-entropy method (CEM) rollouts across forecast scenarios, balancing energy cost minimization, renewable maximization, and asset longevity through an advanced reward shaping mechanism. The agent operates within secure containers using ONNX Runtime and TensorRT for low-latency inference cycles.

AMOS employs a lightweight conceptual MLOps toolchain comprising PyTorch Lightning, TensorFlow Lite, ONNX, OpenVINO, and federated learning orchestrators like Flower. Security and integrity are ensured through Sigstore model artifact signing, and system monitoring is conducted using Prometheus and Grafana dashboards for real-time drift and performance detection.

**4. Security & Ethical Considerations**

AMOS is designed with a rigorous defense-in-depth security posture and strong ethical safeguards.

The system employs cryptographic roots of trust, secure boot, TPM-protected private keys, and SPIFFE-based dynamic device identities. Networks are micro-segmented with VLANs, and telemetry data is encrypted end-to-end using AES-256-GCM.

Integrity validation through Sigstore ensures all model artifacts are verified before execution. Operational resilience is achieved via redundant WAN connections and offline autonomy lasting up to 72 hours. Differential privacy and field-level encryption protect sensitive metrics, ensuring GDPR and NERC-CIP compliance.

Ethical principles are embedded at all layers. Bias mitigation strategies include synthetic augmentation of rare weather and market conditions. Explainability is guaranteed via Shapley value decomposition for every dispatch action. Human-in-the-loop controls are maintained, with operators able to manually override decisions if needed. Federated learning protects data sovereignty, and sustainability goals are supported by minimizing edge inference overhead.

**5. Implementation & Testing Plans (Theoretical)**

AMOS' theoretical deployment follows a structured, secure, and iterative methodology to ensure system integrity, robustness, and operator confidence.

Deployment involves the creation of minimal, hardened operating systems using Buildroot integrated with containerd for lightweight, secure runtime management. Rootless Docker containers host AI models, ensuring strict process isolation. Model training pipelines leverage GitHub Actions for automated validation, conversion (ONNX/OpenVINO), quantization, and artifact signing via Sigstore.

New Edge Gateways auto-enroll securely using SPIFFE-based identity assertions. Configuration secrets are provisioned via tightly controlled Ansible playbooks and Vault-backed encrypted key stores. A Blue/Green deployment strategy ensures that updated models and system images are deployed incrementally, minimizing downtime and allowing automatic rollback if performance KPIs fall outside acceptable thresholds.

Testing covers all critical operational domains:

* **Functional Testing:** Comprehensive scenario validation across 50+ Grid2Op microgrid states ensures that dispatch policies meet operational objectives, including energy efficiency and system resilience.
* **Performance and Stress Testing:** Telemetry ingestion rates exceeding 15,000 points per second are simulated using Locust.io, while real-time dispatch response is monitored to maintain <1-second sense-to-act latencies.
* **Cybersecurity Testing:** Red-team exercises mapped against the MITRE ATT&CK framework are performed to probe for vulnerabilities across segmented networks, ensuring that unauthorized lateral movement is impossible.
* **Fault Tolerance Testing:** Chaos-mesh is used to inject network disruptions, node failures, and black-start recovery scenarios, verifying that AMOS degrades gracefully and restores functionality autonomously.
* **Model Robustness Testing:** Adversarial time-series inputs generated via FGSM perturbations test the resilience of both forecasting and dispatch agents, ensuring that dispatch drift remains within 2% of baseline under attack.
* **Regulatory Compliance Audits:** Mock compliance audits against NERC-CIP, GDPR, IEEE-1547, and DOE C2M2 standards ensure that AMOS meets all necessary regulatory frameworks before going live.

Real-world simulation exercises include black-start drills validating 10-minute system recovery, real-time tariff spike responses optimizing market-facing actions in under 2 minutes, and WAN disconnection survival tests extending 48 hours without operational degradation. Monitoring and alerting are driven by Prometheus metrics and Grafana dashboards, with retraining automatically triggered if KPIs such as forecast MAE or dispatch reward rates degrade beyond set thresholds.

**6. Lessons Learned**

The conceptual design of AMOS revealed several key insights. Achieving low-latency sensing-to-action on constrained edge hardware is feasible with aggressive model optimization and hardware-specific tuning. Embedding physics-informed safety constraints into control policies significantly improves system reliability and compliance.

Maintaining explainability without sacrificing performance requires early integration of decomposition strategies like Shapley value analysis. Continuous online learning and federated model aggregation emerged as essential for ensuring model robustness without compromising privacy. Integrating security at the earliest design phases drastically reduces downstream compliance challenges and operational risks.

**Conclusion**

The Autonomous Microgrid Optimization System represents a cutting-edge convergence of generative AI, reinforcement learning, and edge computing to achieve self-optimizing, resilient, and sustainable energy systems. AMOS provides a practical, scalable blueprint for future autonomous energy infrastructure, emphasizing operational excellence, security, and ethical stewardship. Through careful architectural design, detailed AI model development, robust security frameworks, and thorough testing strategies, AMOS aligns technical innovation with real-world viability. Its design principles can serve as a foundation for broader deployments of AI-driven autonomous agents in critical infrastructure sectors.