LECTURE 20 | المحاضرة 20

Autonomous AI Power Systems

أنظمة القدرة ذاتية التشغيل المدعومة بالذكاء الاصطناعي

A Unified Architecture for Sensing, Reasoning, Optimization, Control, and Safety

معمارية موحدة للاستشعار والاستدلال والتحسين والتحكم والأمان

Autonomy | Architecture | Decision | Safety | Governance | Workflow

Prepared by | إعداد: Dr.-Ing. Aouss Gabash

🎯 Learning Objectives

- Define levels of autonomy in electric power systems.
- Integrate digital twins, GNNs, transformers, RL, RAG, and physics-informed AI.
- Design a perception-reasoning-decision-action loop.
- Separate advisory, supervisory, and closed-loop control functions.
- Construct safety, cybersecurity, and governance layers.
- Evaluate robustness, observability, explainability, and human oversight.
- Formulate a staged roadmap toward autonomous operation.

🎯 أهداف التعلم

- تعريف مستويات الاستقلالية في أنظمة القدرة.
- دمج التوأم الرقمي وGNN وTransformer وRL وRAG والذكاء الموجَّه بالفيزياء.
- تصميم حلقة إدراك واستدلال وقرار وفعل.
- التمييز بين الدعم الاستشاري والتحكم الإشرافي والتحكم المغلق.
- بناء طبقات الأمان والأمن السيبراني والحوكمة.
- تقييم المتانة والرصد والتفسير والإشراف البشري.
- صياغة خارطة طريق تدريجية نحو التشغيل الذاتي.

1. What Does Autonomous Mean?

An autonomous power system senses its state, interprets uncertainty, predicts future conditions, plans actions, verifies constraints, executes approved control, and learns from outcomes.

> Autonomy does not remove engineers. It delegates selected decisions to machines under explicit limits, monitoring, accountability, and safe fallback.

1. ما معنى التشغيل الذاتي؟

يعني أن النظام يقيس حالته ويتنبأ ويخطط ويتحقق من القيود وينفذ القرار المسموح ويتعلم من النتيجة، مع بقاء المسؤولية البشرية.

2. Levels of Autonomy

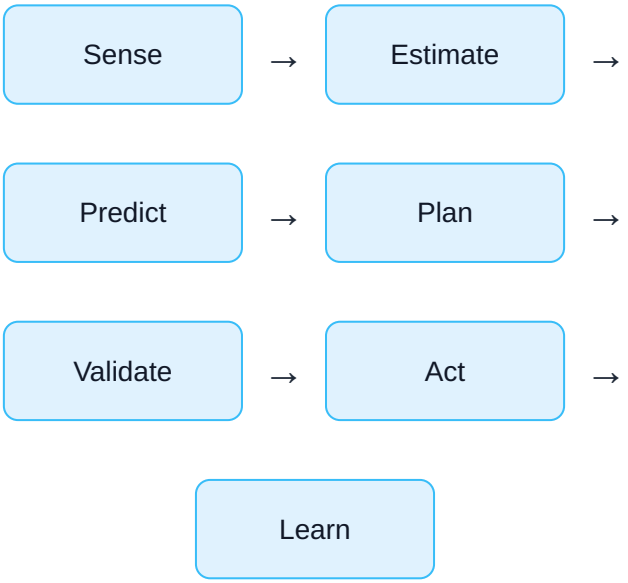
Level	AI Role	Human Role
0	No autonomous function	Full operation
1	Monitoring and alarms	Interpret and act
2	Recommendations	Approve each action
3	Conditional automation	Supervise and intervene
4	High autonomy in a bounded domain	Strategic oversight
5	Full autonomy across conditions	Governance only

Level 5 is a conceptual endpoint; safety-critical deployment should progress through validated bounded domains.

2. مستويات الاستقلالية

تبدأ من المراقبة ثم التوصية والأتمتة المشروطة، وصولًا إلى استقلالية عالية ضمن مجال تشغيل محدد.

3. Autonomous Grid Loop



Each stage must expose confidence, data quality, and failure status to the next stage.

3. حلقة الشبكة الذاتية

تبدأ بالقياس ثم تقدير الحالة والتنبؤ والتخطيط والتحقق والتنفيذ والتعلم من النتيجة.

4. Perception Layer

The perception layer synchronizes SCADA, PMU, smart-meter, relay, weather, market, and asset data.

Temporal AI
LSTM and transformers model time dependencies.

Graph AI
GNNs use electrical topology.

Anomaly Detection
Detect sensor faults and cyberattacks.

Data Quality
Validate timestamps, ranges, units, and missing values.

4. طبقة الإدراك

تجمع القياسات وتوحدها وتتحقق من جودتها وتكشف الأعطال والشذوذ قبل استخدامها.

5. Digital Twin and State Estimation

$$\hat{x}t = Twin(zt, ut, topologyt, parameters)$$

$$z = h(x) + e$$

The twin maintains a synchronized model and supports state estimation, simulation, what-if analysis, and pre-action validation.

The result should include an operating state, confidence bounds, data-quality indicators, and model-health indicators.

5. التوأم الرقمي وتقدير الحالة

يحافظ التوأم على نسخة محدثة للشبكة ويقدم الحالة المقدرة مع مؤشرات الثقة والجودة.

6. Prediction Layer

Load and Renewable Forecasts
Demand, PV, and wind.

Dynamic Security
Transient, frequency, and voltage stability.

Asset Health
Fault risk and remaining useful life.

Market and Congestion
Prices, reserves, and bottlenecks.

$$p(yt+h|x1:t,u1:t)$$

6. طبقة التنبؤ

تتوقع الأحمال والمتجددة والاستقرار وصحة المعدات والأسعار والاختناقات.

7. Decision Layer

$$u* = argminuJ(x,u)$$

$$s.t.g(x,u) \leq 0, h(x,u) = 0$$

$$uRL = \pi\theta(s)$$

Optimization, MPC, reinforcement learning, rules, and expert knowledge can work together.

> A practical architecture uses AI for prediction, approximation, prioritization, or policy selection, while deterministic optimization and physics provide guarantees.

7. طبقة القرار

تجمع بين التحسين وMPC وRL والقواعد، مع إبقاء الضمانات الفيزيائية والحتمية قبل التنفيذ.

8. Multi-Agent and Federated Intelligence

$$xi(k+1) = \sumjwijxj(k)$$

$$wglobal = \sumk(nk/N)wk$$

Multi-agent coordination supports distributed control, while federated learning enables collaborative model training without centralizing raw data.

Both approaches require communication security, resilience to malicious participants, and fallback local operation.

8. الذكاء متعدد الوكلاء والاتحادي

يدعم الأول التحكم الموزع، بينما يسمح الثاني بتدريب نماذج مشتركة دون جمع البيانات الخام.

9. Generative AI and RAG Assistants

Language-model assistants can retrieve procedures, explain alarms, summarize events, generate code prototypes, and draft reports.

An LLM should not directly command critical equipment without source grounding, tool validation, access control, deterministic safety checks, and explicit authority boundaries.

9. المساعدات التوليدية وRAG

يمكنها استرجاع الإجراءات وشرح الإنذارات وكتابة التقارير، لكن لا ينبغي أن تتحكم مباشرة بالمعدات الحرجة دون ضوابط صارمة.

10. Safety Filter

$$usafe = argminu\|u - uAI\|^2$$

$$s.t.voltage, thermal, frequency, reserve, ramp, storage, protection, \quad \text{and} \quad N-1constr$$

Every proposed action passes a deterministic feasibility layer before execution.

10. مرشح الأمان

يمر كل قرار عبر طبقة تحقق حتمية تفرض الحدود التشغيلية والحماية ومعيار N-1.

11. Human-in-the-Loop

Advisory Mode
AI explains and recommends.

Approval Mode
A human authorizes each action.

Supervisory Mode
AI acts inside a bounded envelope.

Emergency Override
Human or protection can stop autonomy.

Authority should be proportional to validated capability, operating risk, and uncertainty.

11. الإنسان ضمن الحلقة

قد يكون النظام استشاريًا أو يحتاج موافقة بشرية أو يعمل ضمن مجال محدود مع إمكانية الإيقاف الطارئ.

12. Physics-Informed Autonomy

$$Jtotal = Jdata + \lambda pfJpower - flow + \lambda dynJdynamics + \lambda limJlimits$$

Physics-informed models reduce impossible states and actions, but the underlying model and parameters must also be validated.

12. الاستقلالية الموجَّهة بالفيزياء

تدمج الخسارة اتزان القدرة والديناميكا والحدود التشغيلية لتقليل النتائج غير الفيزيائية.

13. Uncertainty and Risk

$$Risk(a) = \sum \omega P(\omega) \cdot Loss(a, \omega)$$

$$P(g(x, u) > 0) \leq \varepsilon$$

Autonomous decisions should account for forecast error, model uncertainty, sensor failure, and topology ambiguity.

When confidence is insufficient, the system should reduce authority, request human review, or enter a safe fallback mode.

13. عدم اليقين والمخاطر

يجب احتساب أخطاء التنبؤ والنموذج والحساسات والطوبولوجيا، وتقليل صلاحية النظام عند انخفاض الثقة.

14. Cybersecurity and Resilience

- Zero-trust identity and least privilege.
- Signed models and secure update channels.
- Anomaly detection across cyber and physical signals.
- Redundant sensing and communication.
- Local fallback controllers.
- Incident response, rollback, and recovery.

14. الأمن السيبراني والمرونة

تتطلب الاستقلالية هوية موثوقة وتحديثات آمنة ومراقبة مستمرة وتحكمًا احتياطيًا وخطة تعافٍ.

15. Explainability, Auditability, and Governance

Explainability
Why was an action proposed?

Auditability
Which data, model, and rules were used?

Accountability
Who owns the final decision?

Change Control
How are models validated and released?

Every high-impact decision should retain inputs, model version, confidence, constraints, explanations, approvals, and final outcome.

15. التفسير والتدقيق والحوكمة

يجب حفظ البيانات والنموذج والثقة والقيود والشرح والموافقة والنتيجة لكل قرار عالي الأثر.

16. Validation Framework

1. Software-in-the-loop testing.
2. Hardware-in-the-loop testing.
3. Historical event replay.
4. Rare-event and adversarial scenarios.
5. Communication failure and missing-data tests.
6. Shadow-mode operation without control authority.
7. Limited pilot deployment with rollback.

Autonomy should earn authority through evidence collected at progressively more realistic validation stages.

16. إطار التحقق

يبدأ بالمحاكاة ثم الاختبارات العتادية وإعادة الأحداث ووضع الظل والتجارب المحدودة قبل منح صلاحية أكبر.

17. Key Performance Indicators

Reliability
Unserved energy and interruption metrics.

Safety
Constraint violations and near misses.

Economy
Cost, losses, and renewable utilization.

Autonomy Quality
Interventions, overrides, and fallback frequency.

Robustness
Performance under faults and attacks.

Trust
Explanation quality and operator acceptance.

17. مؤشرات الأداء

تشمل الموثوقية والأمان والاقتصاد وجودة الاستقلالية والمتانة وثقة المشغل.

18. Engineering Roadmap

Define Bounded Use Case → Build Twin & Data Layer → Train AI → Add Safety & Governance → Validate & Expand

1. Select a narrow, measurable operational use case.
2. Define authority limits and fallback behavior.
3. Build synchronized data and digital-twin foundations.
4. Integrate prediction, optimization, and safety filtering.
5. Validate in simulation, shadow mode, and limited pilots.
6. Increase authority only after documented evidence.

18. خارطة الطريق الهندسية

نبدأ بحالة استخدام محدودة، ونبني البيانات والتوأم، ثم نضيف الذكاء والأمان والحوكمة ونوسع الصلاحيات تدريجيًا.

🔬 Research Corner

Emerging directions: foundation models for power systems, world models, autonomous restoration, safe multi-agent RL, neuro-symbolic reasoning, self-healing digital twins, and verified AI control.

🔬 زاوية البحث العلمي

تشمل الاتجاهات الحديثة النماذج الأساسية ونماذج العالم والاستعادة الذاتية وMARL الآمن والاستدلال العصبي الرمزي والتحكم المتحقق منه.

🧠 Review Questions

1. What distinguishes advisory AI from autonomous control?
2. Describe the autonomous grid loop.
3. How do digital twins support autonomy?
4. Why is a deterministic safety filter needed?
5. How should uncertainty affect control authority?
6. What is the role of humans at different autonomy levels?
7. How should autonomous systems be validated?
8. What evidence is required before increasing autonomy?

🧠 أسئلة المراجعة

1. ما الفرق بين الذكاء الاستشاري والتحكم الذاتي؟
2. اشرح حلقة الشبكة الذاتية.
3. كيف يدعم التوأم الرقمي الاستقلالية؟
4. لماذا نحتاج مرشح أمان حتميًا؟
5. كيف يؤثر عدم اليقين في صلاحية التحكم؟

6. ما دور الإنسان في مستويات الاستقلالية المختلفة؟
7. كيف نتحقق من الأنظمة الذاتية؟
8. ما الأدلة المطلوبة قبل زيادة الصلاحيات؟

References | المراجع

المراجع العامة المستخدمة في هذا المقرر

[1] A. Gabash, *Flexible Optimal Operations of Energy Supply Networks with Renewable Energy Generation and Battery Storage*. Saarbrücken, Germany: Südwestdeutscher Verlag für Hochschulschriften, 2014.

[2] S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th Global ed. Harlow, U.K.: Pearson Education Limited, 2022.

[3] A. Gabash, “Energy Market Transition and Climate Change: A Review of TSOs-DSOs C+++ Framework from 1800 to Present,” *Energies*, vol. 16, no. 17, Art. no. 6139, 2023, doi: 10.3390/en16176139.

[4] A. Gabash, *AI Applications in Electrical Power Systems*, Version 1.0, 2026. [Online]. Available: https://aoussgabash.com

Publication Information | معلومات النشر

Document	Lecture 20 · Autonomous AI Power Systems
Course	AI Applications in Electrical Power Systems
Author	Dr.-Ing. Aouss Gabash
Version	1.0
Publication year	2026
Official website	https://aoussgabash.com
Citation style	IEEE

Recommended citation:

Gabash, A. (2026). Autonomous AI Power Systems. AI Applications in Electrical Power Systems, Lecture 20, Version 1.0. https://aoussgabash.com

المرجع المقترح:

أوس غباش، 2026، محاضرة 20، تطبيقات الذكاء الاصطناعي في أنظمة الطاقة الكهربائية، الإصدار 1.0، https://aoussgabash.com

© 2026 Dr.-Ing. Aouss Gabash. Educational use with attribution to the author and official website.