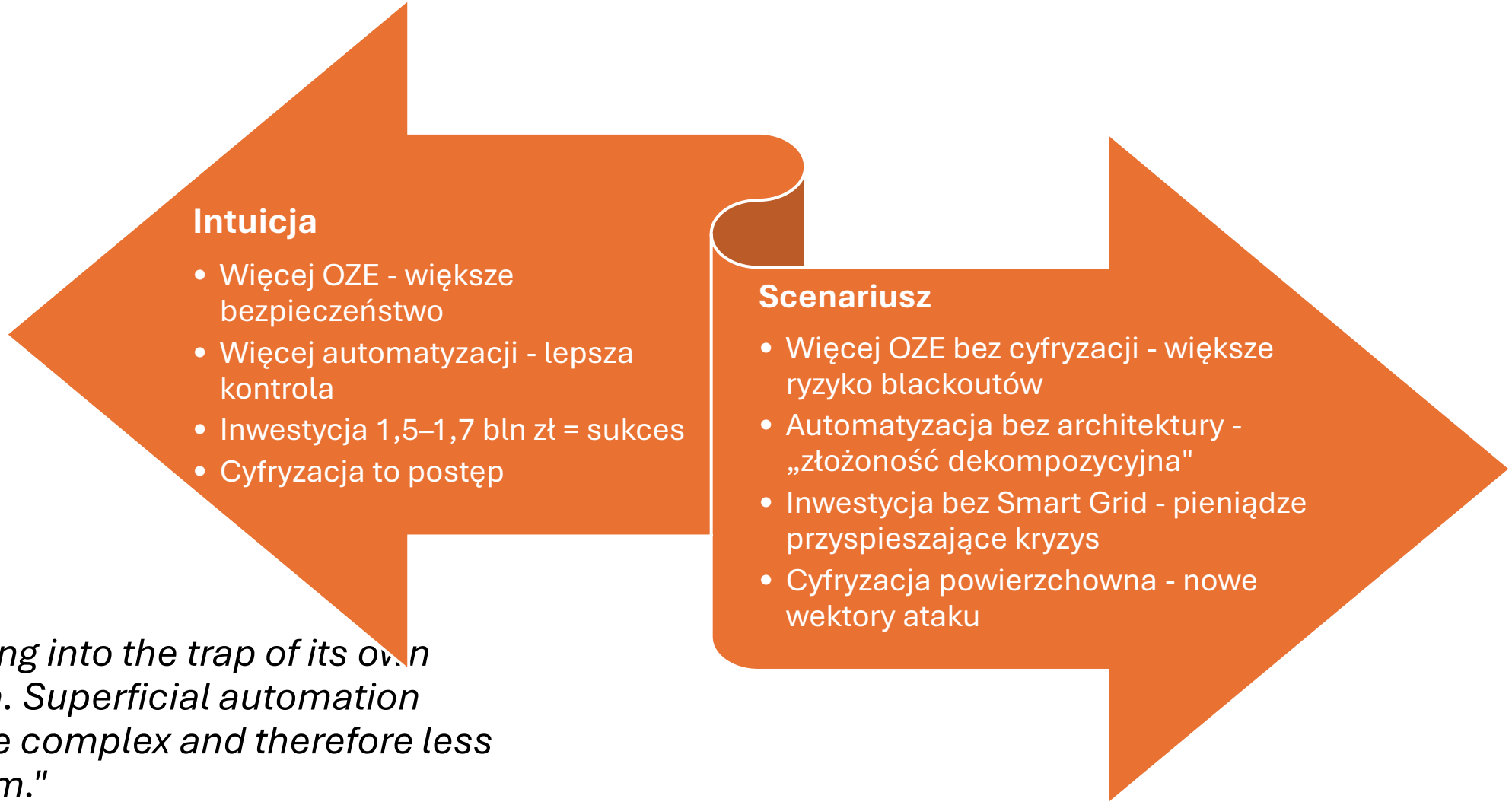
Polish Digital Resilience Agenda 2040
a model of strategic preparedness
for the antinomies of digitalisation.

Scenario: Systemic instability

strategic area: Energy

Anatomy of the digital fragility of the Polish energy sector until 2040

The main paradox: modernization as a source of threat



"Poland is falling into the trap of its own modernization. Superficial automation creates a more complex and therefore less resilient system."

Vulnerability spiral

Phenomenon	Effect
No predictive analytics (24-72h RES)	Operating costs +15-20%, excess power reserves
No automatic 50 Hz adjustment	Risk of blackouts +35-45%
Prosumer chaos (3–5 million installations by 2040)	Millions of unsynchronized sources = network destabilization
"Tower of Babel" - Lack of interoperability	Data silos, integration costs increase to 7% vs. target 1.6%
IT technical debt	Each year of delay = transformation costs +3-5% (PLN 150-250 billion by 2040)
Underinvested in cybersecurity	Infrastructure attacks: +340% (2019-2024), 68% via legacy vulnerabilities
Competence gap	Outflow of IT specialists → return to error-prone manual procedures

Digital fragility and decompositional complexity

Decompositional complexity – example:

Traditional grid (2000):

Power station A – Grid
Power station B – Grid
Power station C – Grid
[Operator SEES the system]

The grid in 2035 without a Smart Grid:

3 million prosumers
450 wind farms
200 PV farms
Millions of electric vehicles
[Operator is DROWNED in data]
[NO ONE sees the whole picture]

Digital Fragility: A condition in which increases in technological complexity outpace increases in system resilience. Instead of self-healing - cascading failures.

Effects:

Brownouts

localised voltage drops as the 'new normal'

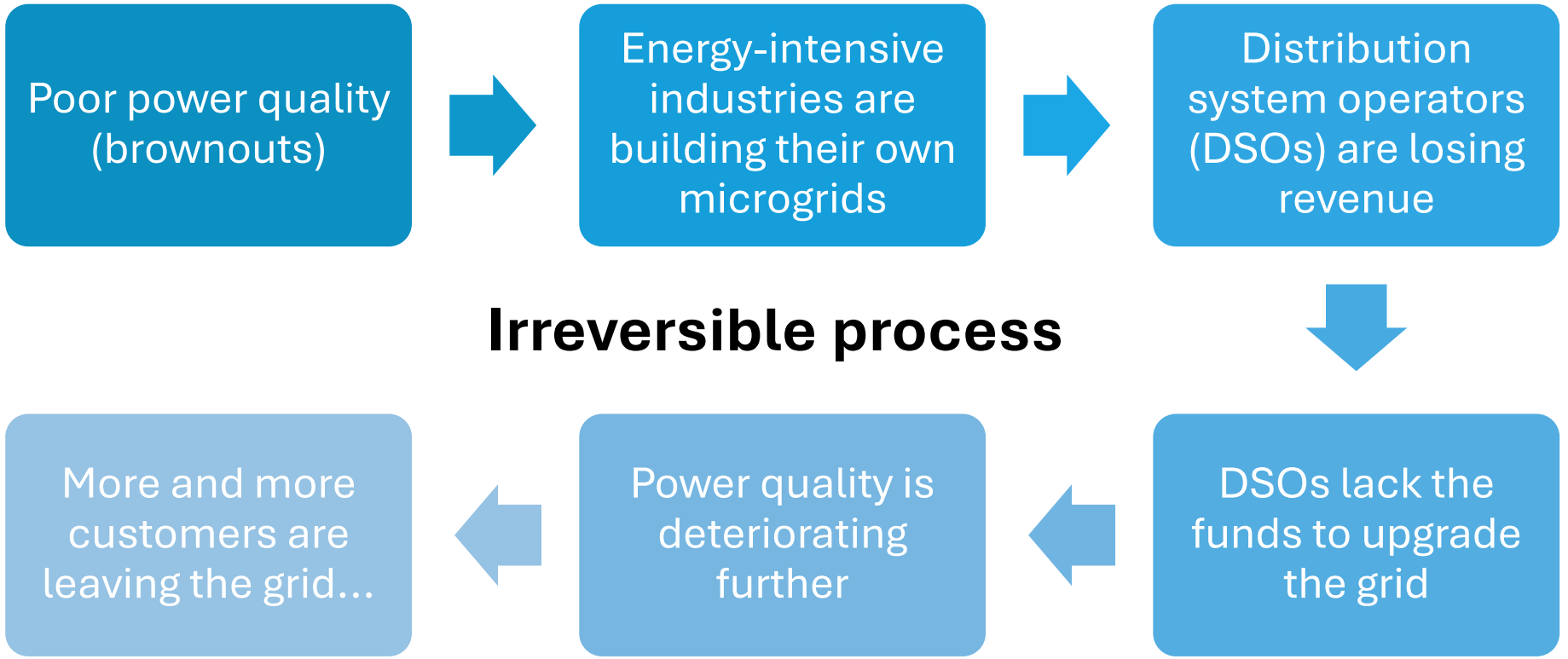
Cascading blackouts

a failure at a single node triggers a chain reaction

Data overload in control centres

operators are unable to keep up with the decisions

Grid Defection spiral



Systemic consequence:

- System balancing costs: significantly higher than in a digitally stable system
- Renewable energy integration costs: instead of falling, they remain at the same level

Cybersecurity: Dramatic escalation of threats

Increase in attacks 2019–2024	Attacks exploiting vulnerabilities in legacy systems	Probability of cascading failures	OT cybersecurity readiness
+340%*	68% of all incidents	+35–40% over a 15-year period	2.1 / 5 (NIST)

Potential sources of threats:

- **Hostile states**
  - attacks on critical infrastructure as acts of war
- **Criminal groups**
  - ransomware targeting SCADA systems (precedent: Colonial Pipeline, USA)
- **Quantum threats**
  - future compromise of current cryptography

*ENIS Report (2024)

Economic calculation of the crisis

Total planned investments

- 1,5–1,7 bln PLN

Renewable energy sources

- 600 mld PLN

Additional costs associated with technical debt

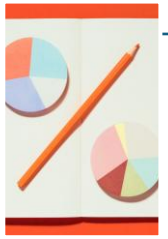
- +150–250 mld PLN to 2040

The annual cost of delay

- 3–5% costs of transformation

Higher operating costs

- +15–20% vs. a mature system



Higher balancing costs

- +40–60% vs. digital system

Grid defection — loss of revenue for the DSO

- An irreversible spiral

Key conclusion: Poland may spend PLN 1.7 trillion and worsen system stability if digitalisation remains superficial

Recommendations: four imperatives

The imperative of integration

mandatory interoperability standards for the entire sector; an end to the 'Tower of Babel'

Cybersecurity as a cornerstone

OT protection on a par with the physical security of power stations; treated as a component of national defence

Investment realism

the expansion of renewable energy must be synchronised with the roll-out of the Smart Grid; a ban on 'non-intelligent grids'

Human capital

closing the hybrid skills gap (IT + energy), eliminating 'data overload' for control centre operators

Operation window:
Each year of delay amounts to 3-5% of the transformation costs. At the current rate of maturity growth, disaster by 2040 is statistically certain.

Conclusion

“There is nothing more dangerous than modernization without foundations - because it gives the illusion of security that does not exist.”



Ministerstwo Nauki
i Szkolnictwa Wyższego

Polish Digital Society
http://cyfryzacja.org

The project is financed from state budget funds allocated by the Minister of Education and Science under the "Science for Society II" Program._x000B_Funding: PLN 1,467,000, Total value: PLN 1,467,000

Postscript: one-page script

This is the most dangerous scenario in the energy series — and the subtlest. This is the story of an active catastrophe caused by action — a modernization that destroys more than inaction. Poland falls into the trap of its own modernization.

The paradox is precise and terrifying: we are investing PLN 1.5-1.7 trillion in the energy transformation. We build wind farms in the Baltic Sea, install millions of photovoltaic panels, and connect millions of prosumers. And this effort – if not based on a mature digital architecture – turns into a weapon turned against us. The system becomes more complex, more dependent on digitalisation, but digitalisation remains superficial, fragmented, inconsistent. Effect: the more renewable energy sources, the more chaos.

The mechanism is called “decompositional complexity” — the system becomes too complex for its own control tools. It's like building successive floors of a skyscraper on the foundations of a house of cards. Each new renewable energy floor is just such a floor. With three million prosumers, no common management platform, no 50 Hz automatic frequency regulation, no 24-72 hour predictive analytics — the network can't see itself. Operators are drowning in data they cannot process. A "new normal" is emerging: brownouts, cascading blackouts, information overload failures.

The exit from the system - "grid defection" - completes the spiral: the energy-intensive industry flees to its own microgrids, taking with it the revenues of distribution operators, who therefore do not have the funds for modernization, which causes the quality of energy to decline further, causing subsequent consumers to flee. The loop closes.