URBAN WATER MANAGEMENT AND HYDROINFORMATICS GROUP

ISSRI Institute for Smart, Sustainable & Resilient Infrastructure

NATIONAL TECHNICAL UNIVERSITY OF ATHENS

Cyber-Physical Water Infrastructure under Climate Extremes and Human Threats

Christos Makropoulos

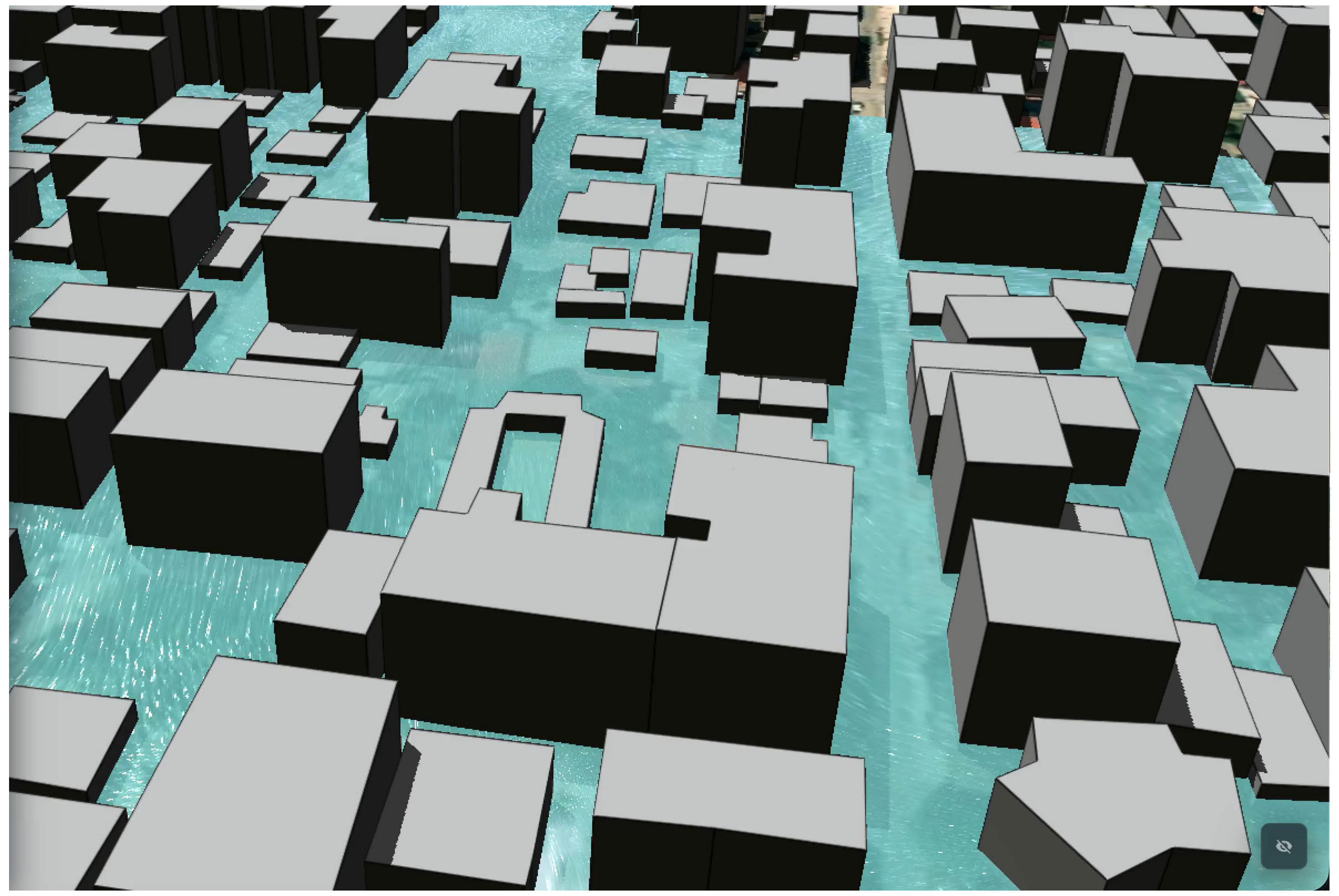
Professor, School of Civil Engineering

Director, Laboratory of Applied Hydraulics

Director, Institute of Smart, Sustainable and Resilient Infrastructure

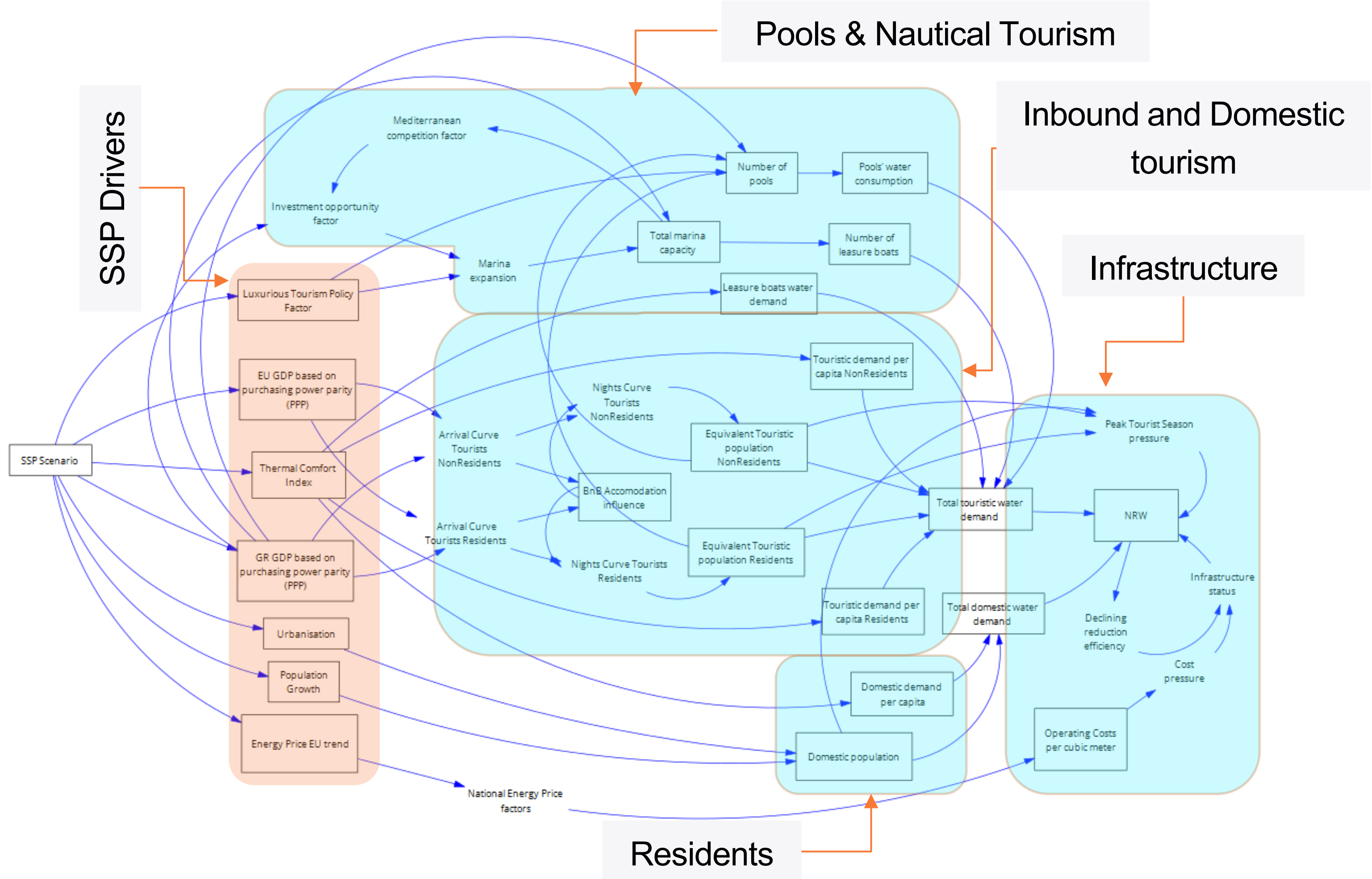
The starting point: making water systems more "intelligent" under uncertainty

Water as an "environment"



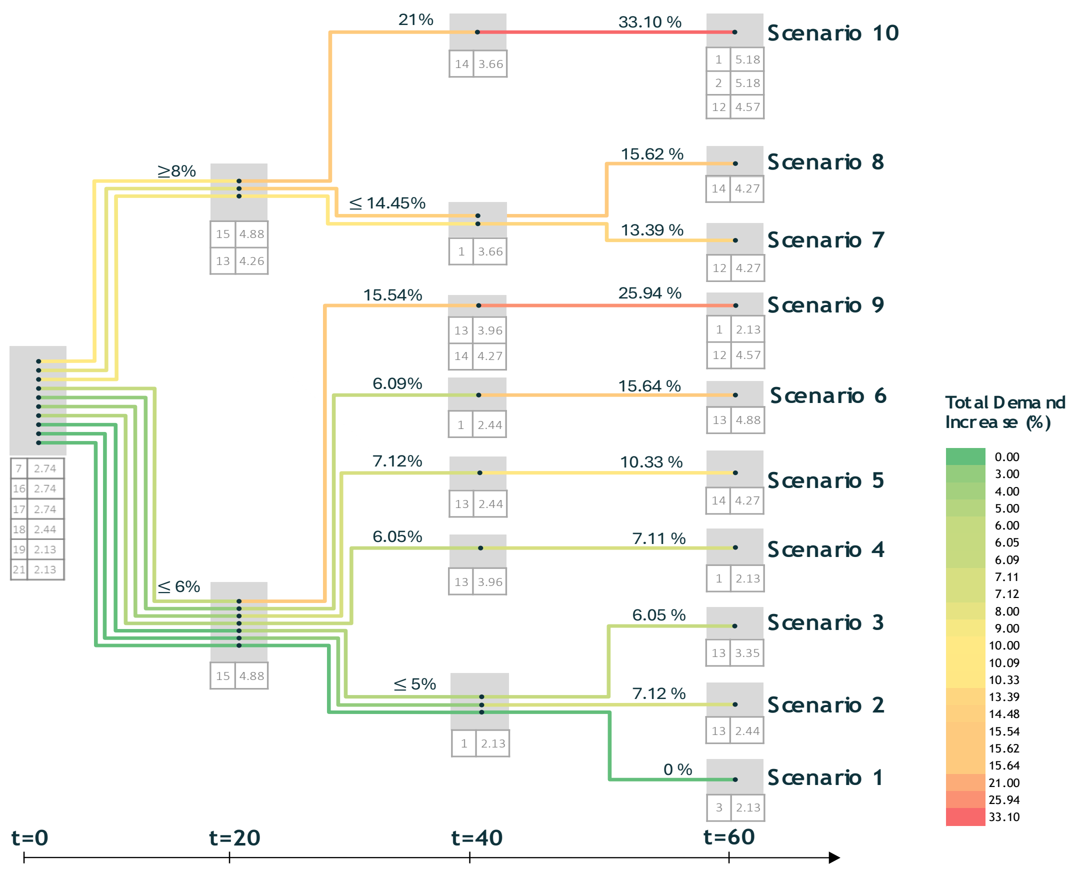
Combined Hydrologic & Hydrodynamic simulation of **extreme floods** (Ianos & Daniel in Thessaly): learning from event reconstruction.

Water as a "resource"

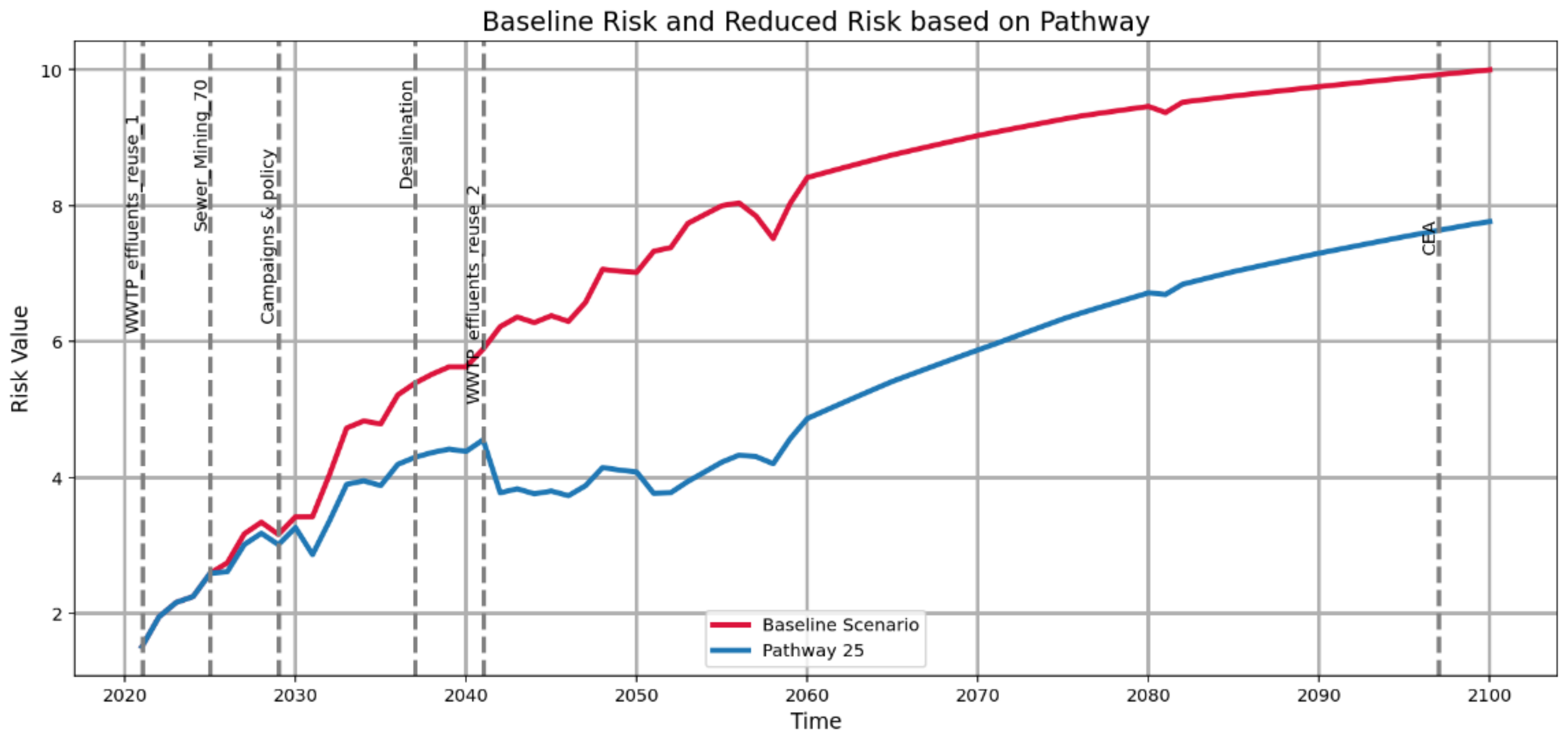


Water system options under different dynamic future scenarios for Syros: **alternative water resources** (reuse, desal, gw) utilisation for increased resilience

Water as "infrastructure"



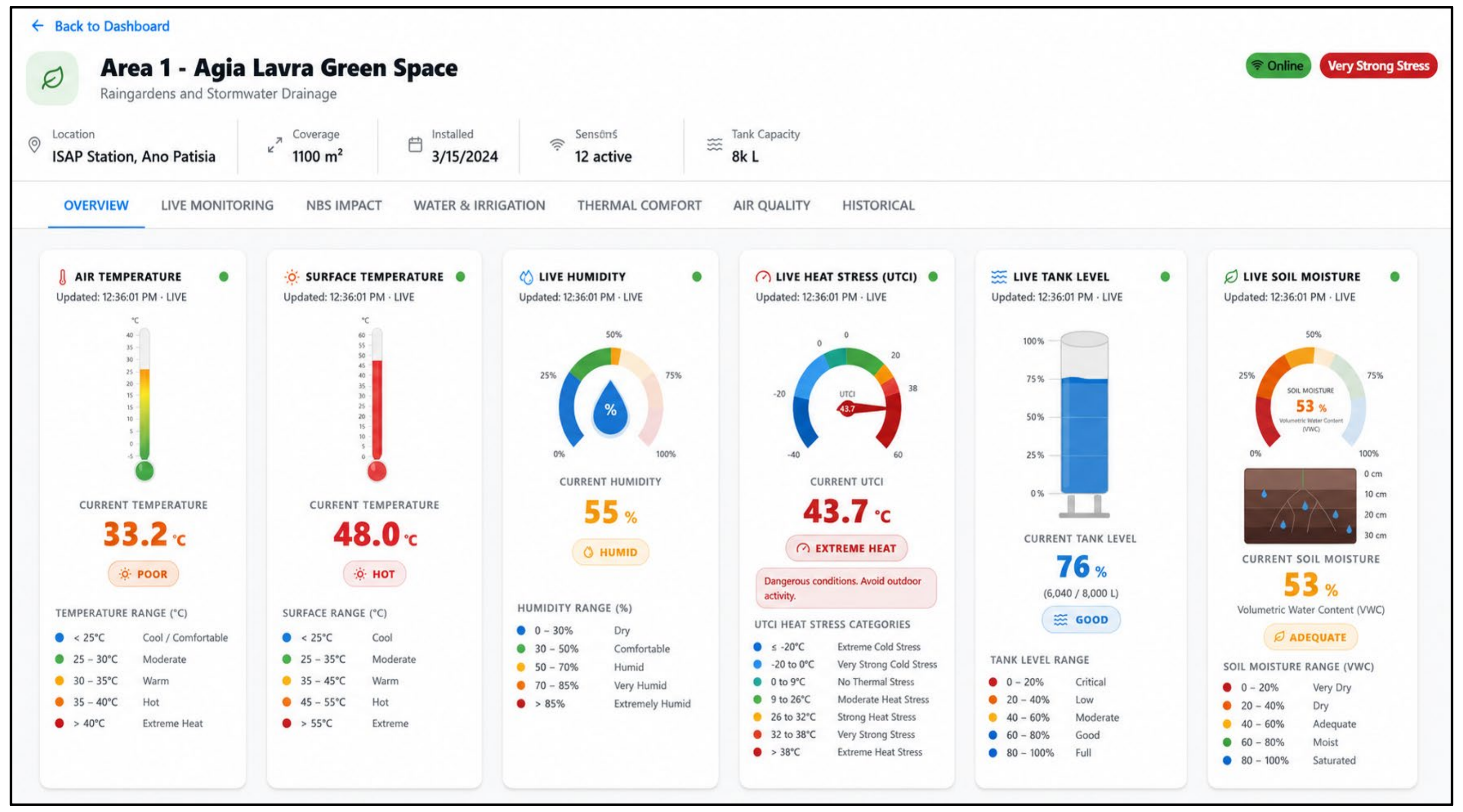
Deep reinforcement learning framework for **flexible water distribution network** design under deep uncertainty.

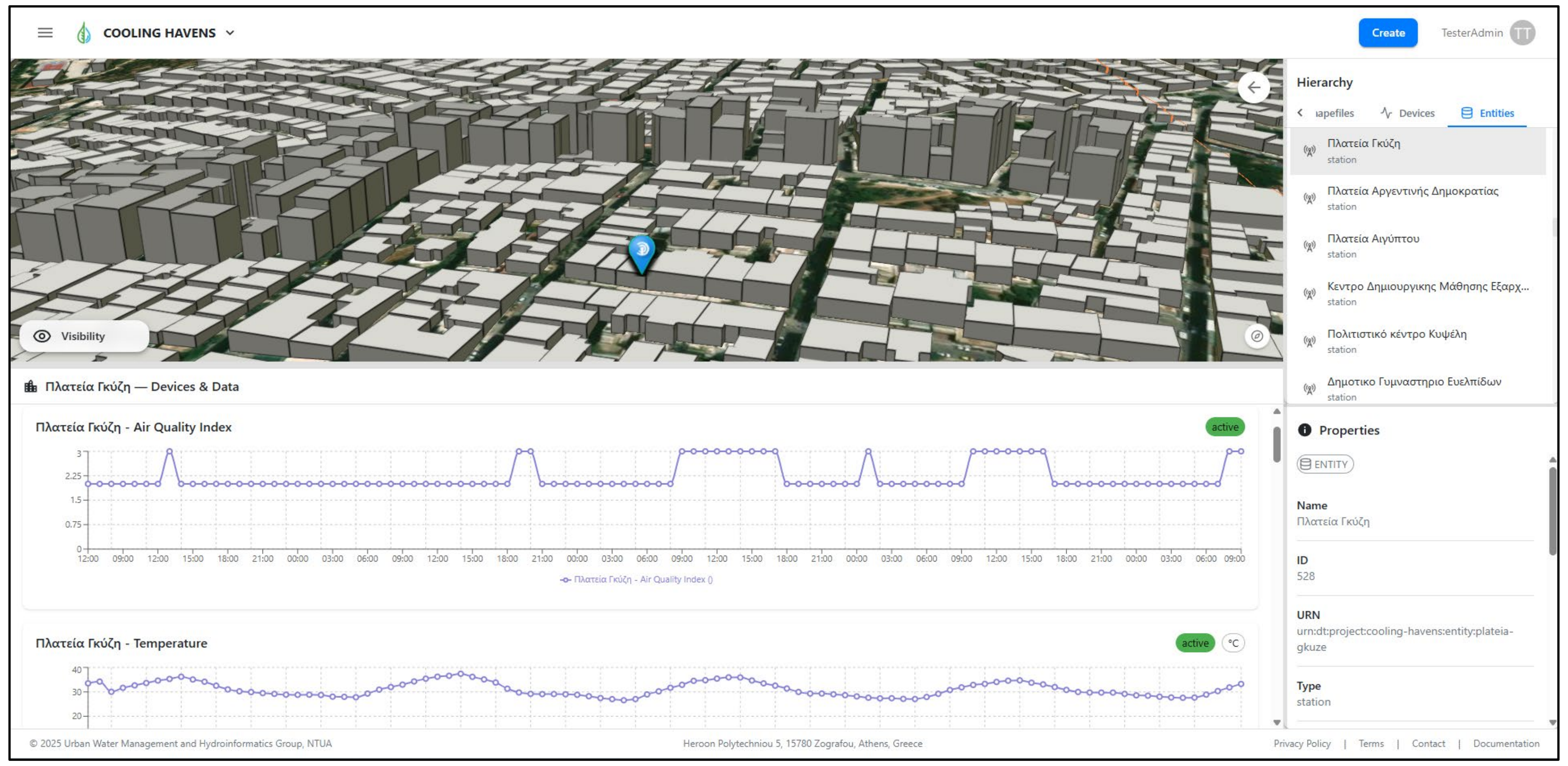


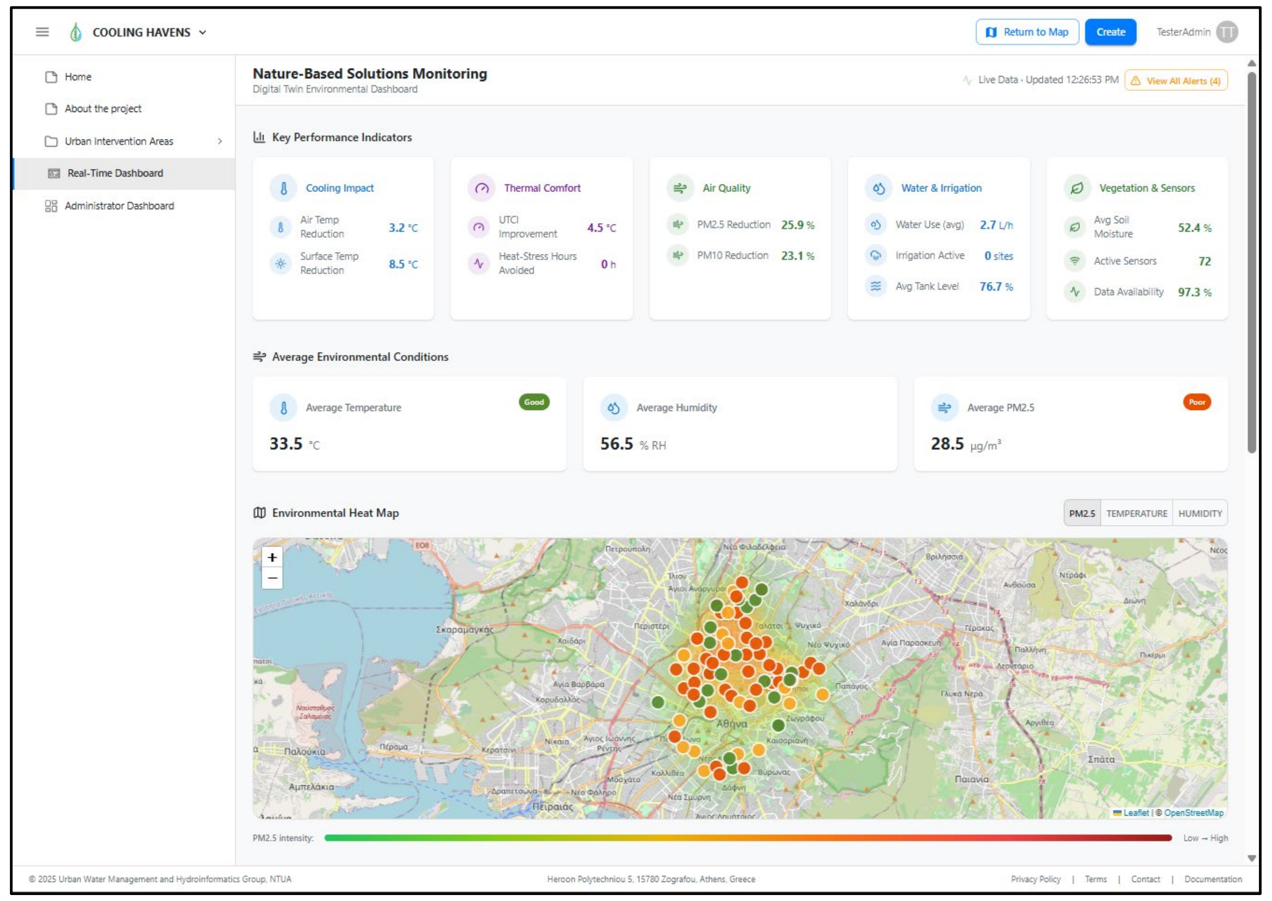
Calculate **adaptation pathways** under **deep uncertainty**, where alternative sequences of interventions (central/decentral – structural/policies) are evaluated against **multiple plausible futures** and triggered by adaptation **tipping points** (rather than fixed scenario assumptions).

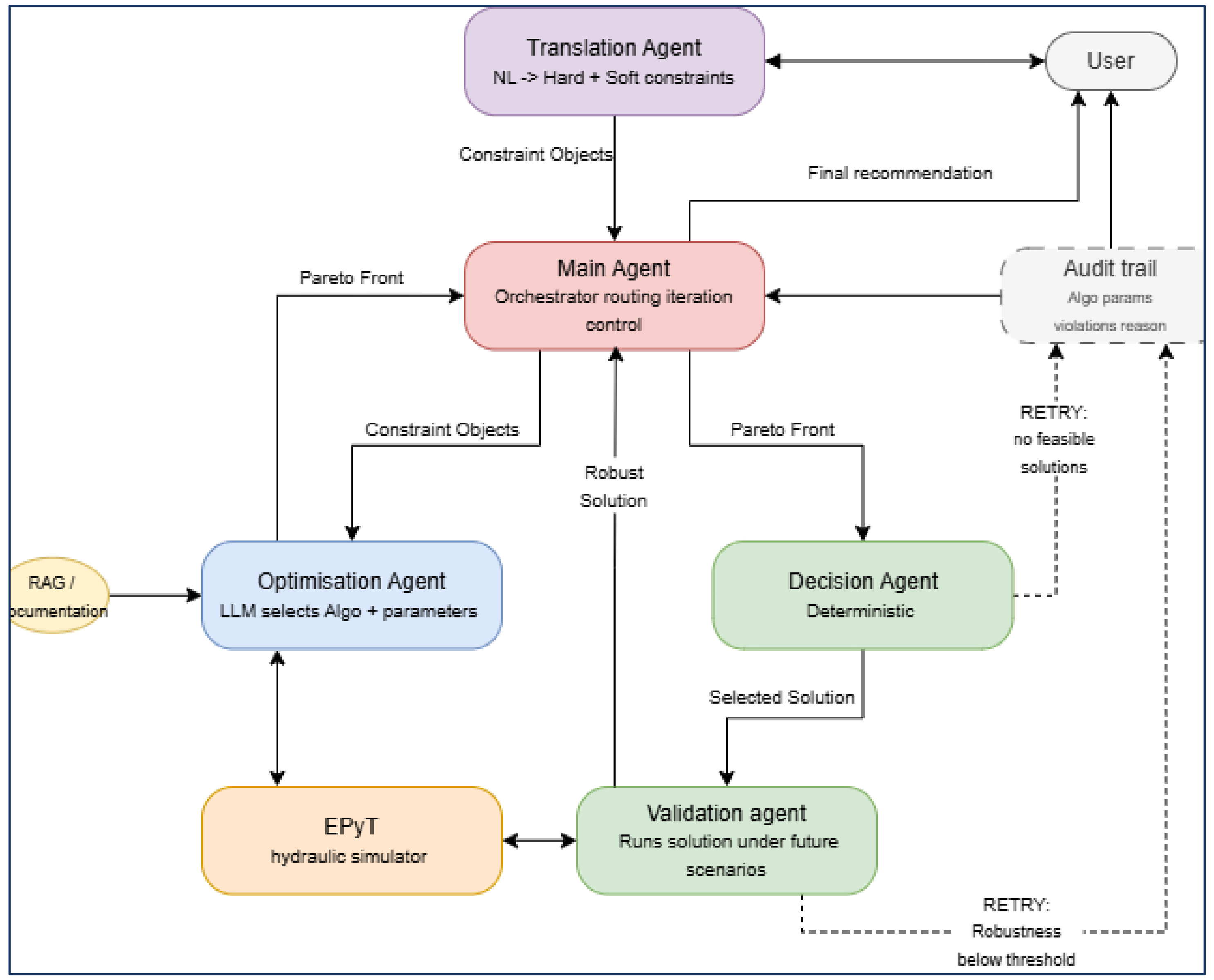
ISSRI Institute for Smart, Sustainable & Resilient Infrastructure

And our tools are becoming more integrated: DTs and Agentic AI









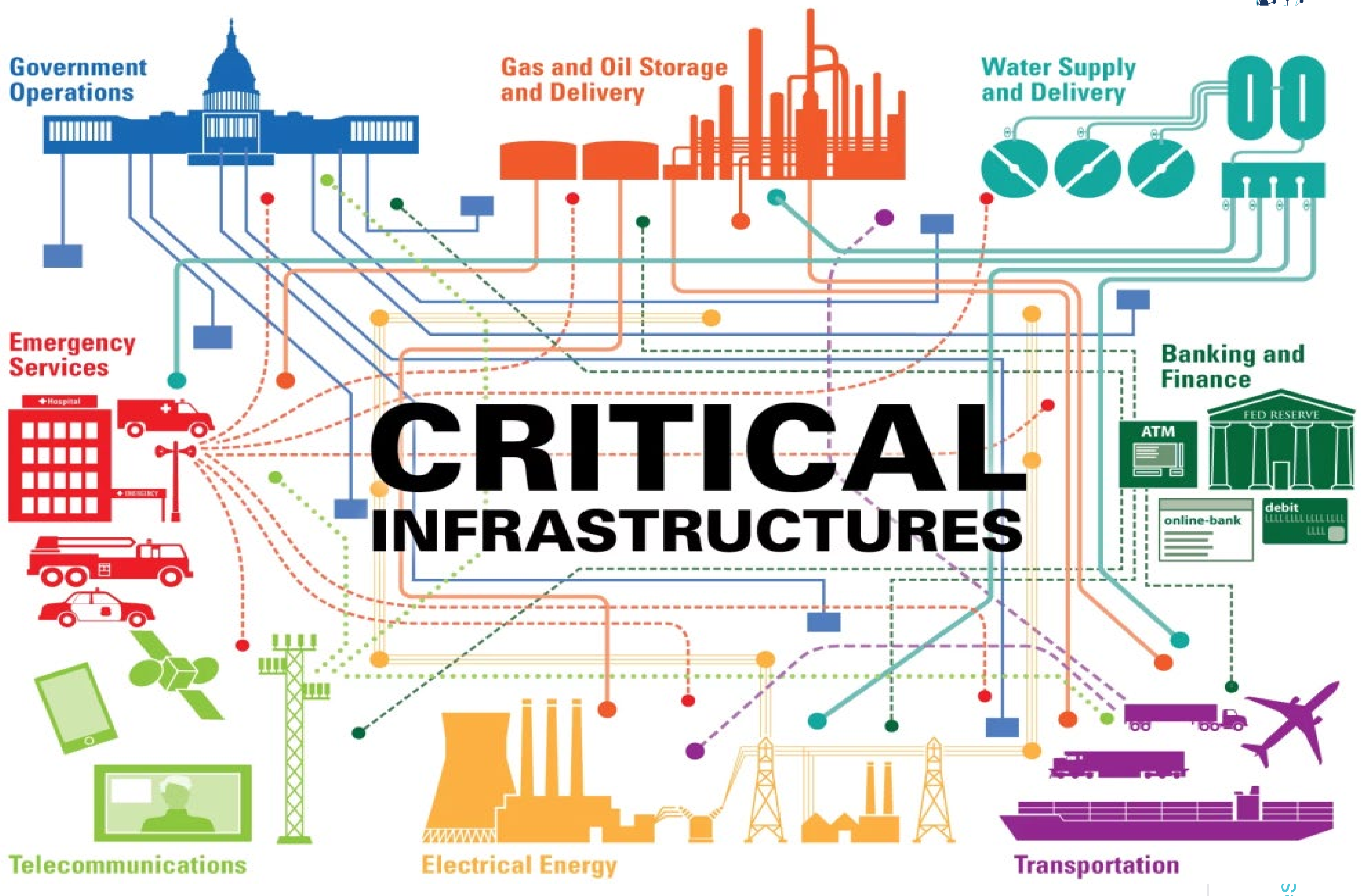
Digital Twins are increasingly where our **toolchains become available for decision-making**: we use them as digital infrastructure to **connect** GIS, EO products and IoT with hydrologic and hydraulic simulations, classic ML, indicators and metrics for “whole lifecycle” support of (often hybrid) infrastructures.

We are also starting to experiment with **AI Agents,** orchestrating workflows, connecting models/evidence, explaining solutions, validating and stress-testing designs.

Although not acting on the real water system (yet).

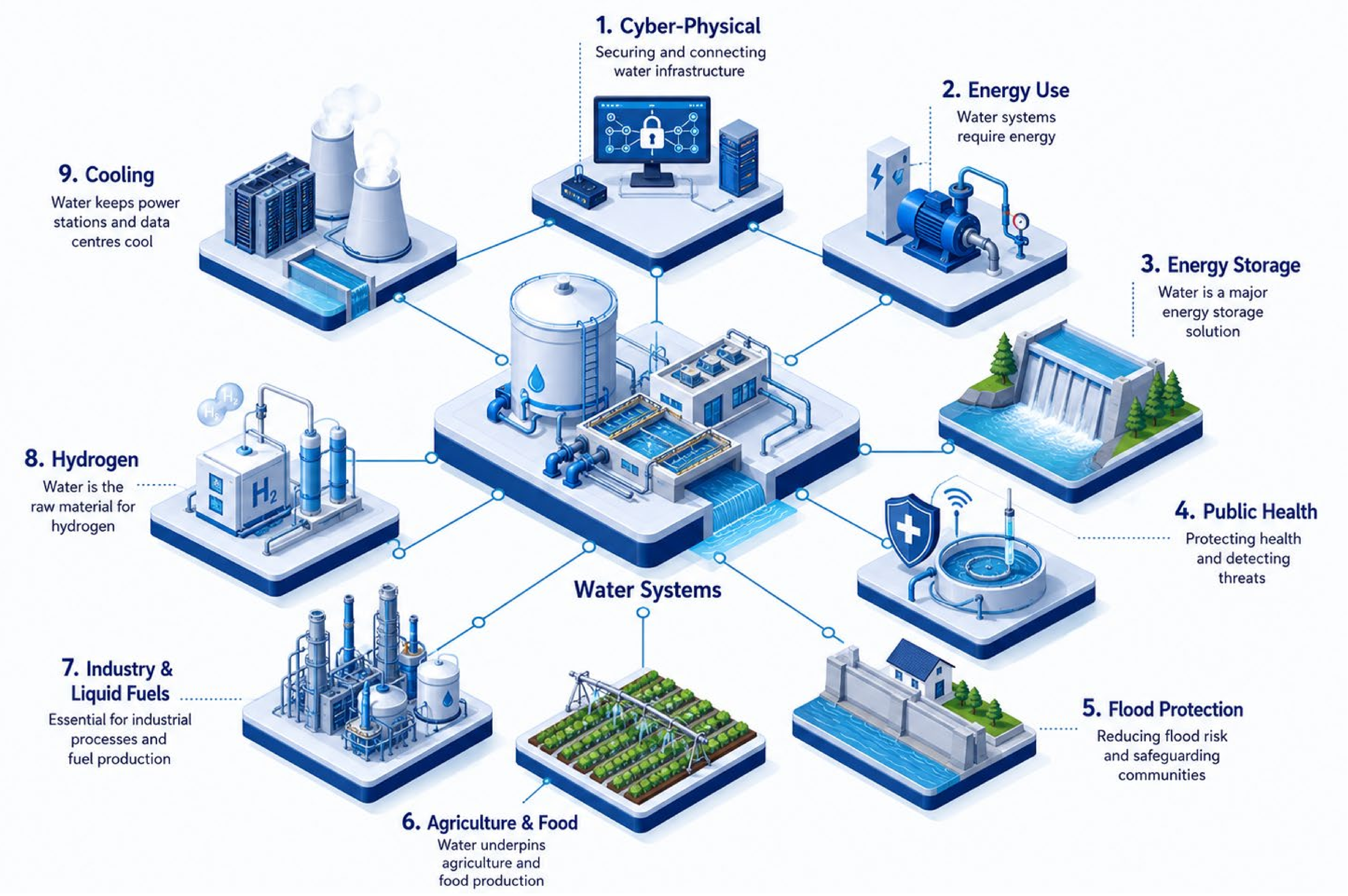
The boundary of the “water system” is no longer the water utility

- As water systems become intelligent, connected and automated, their **dependencies become visible**: energy, telecoms, computing power, transport, supply chains and people.
- At the same time, the **operating context has shifted**: chronic **underinvestment**, climate **extremes**, **geopolitical pressure**, **cyber** threats, and **hybrid/NaTech** hazards are no fringe occurrences – they are part of the “**new normal**”.



So, water is not a standalone sector — it is part of a wider domino...

- Water systems are coupled to cyber-control layers, creating an extended attack surface.
- They need energy for pumping, treatment and automation.
- Energy needs water for hydropower, cooling and storage (especially as RES penetration increases).
- Public health needs water for safety, sanitation and surveillance.
- Cities need water infrastructure for flood protection.
- Food, industry, defence, fuels and hydrogen **all need water** as a critical resource.



Case in point: Data Centres also need a lot of water!

Rack heat → Cold plate / DLC → Coolant loop → Heat exchanger → Dry / hybrid rejection

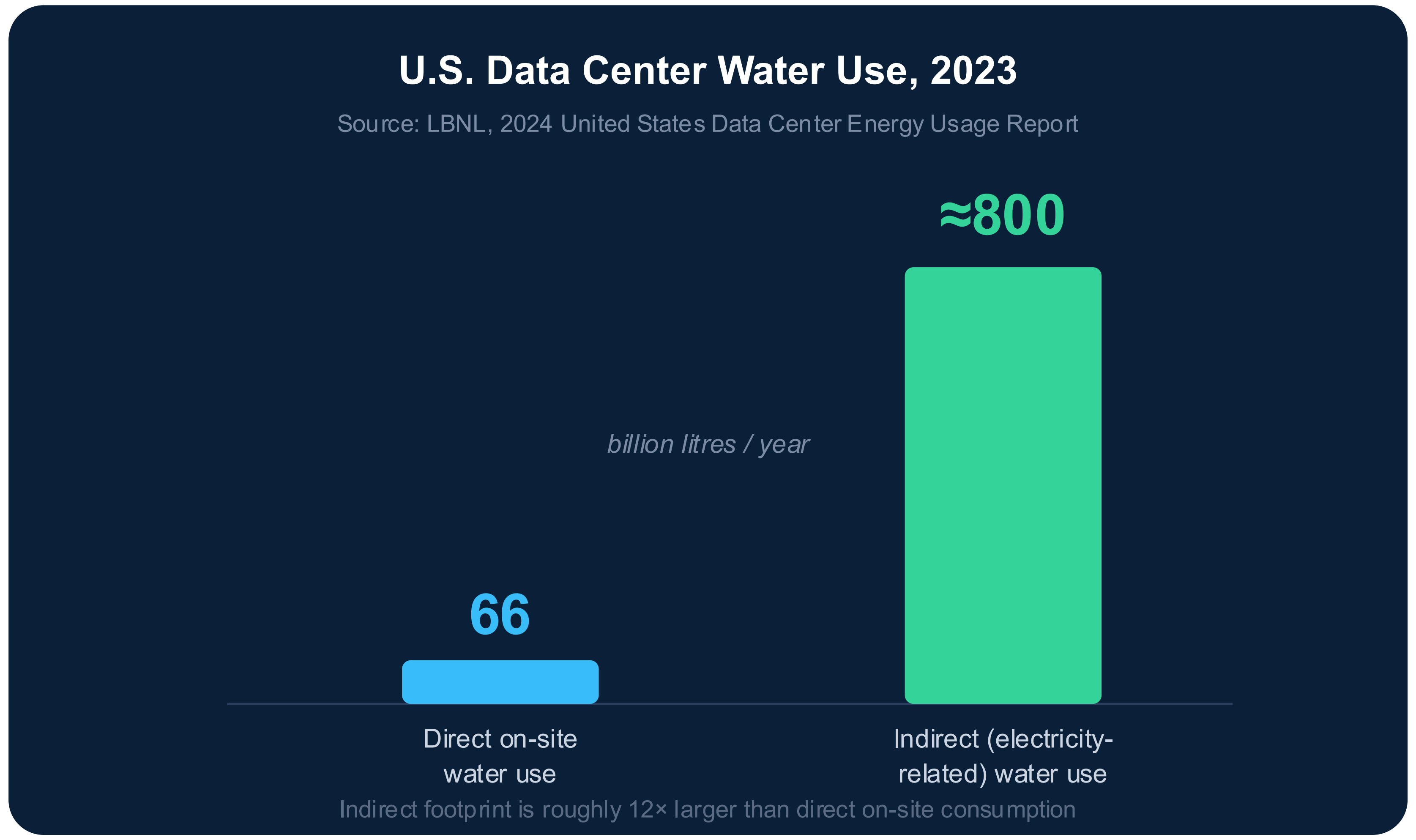
Failure modes

pump failure; heat-exchanger fouling; air-side dust/salt; leak detection; coolant contamination; control instability

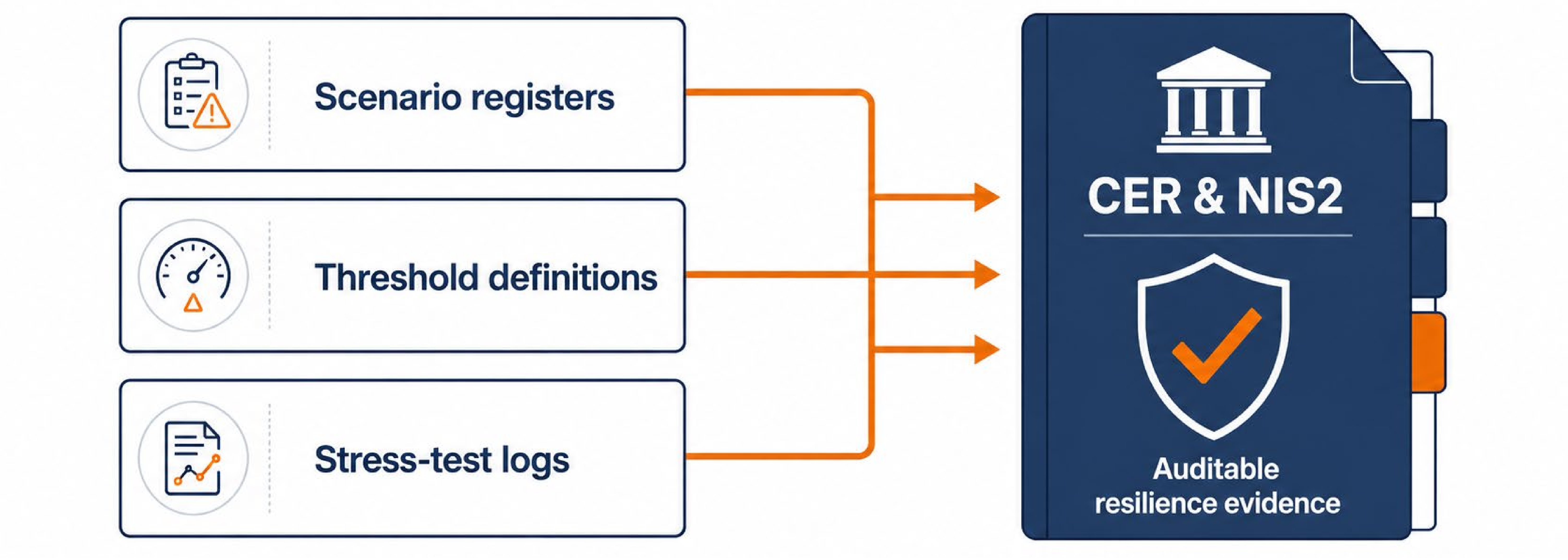
Operational levers

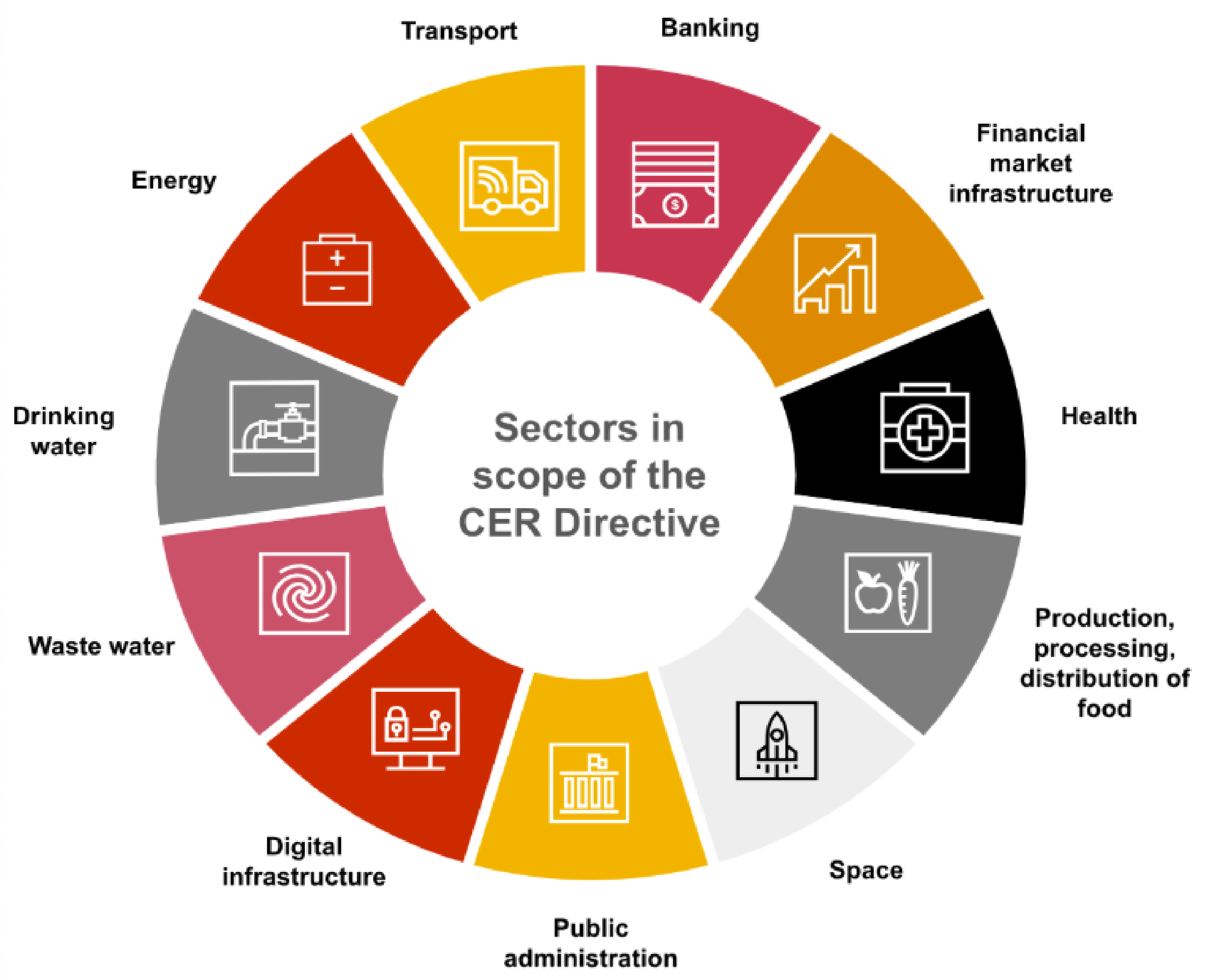
workload shedding; setpoint adjustment; thermal buffering; coolant treatment; dispatchable power; water prioritisation

- Direct liquid cooling is **a water management problem**: chemistry, filtration, monitoring and spare parts for the water system become critical for data centre operation.
- In fact, **water exposure of Data Centres** should be assessed through several dimensions: **facility cooling** water, water need for **electricity production** and **water quality** required to keep the thermal systems available.



Regulation is emerging - asking for resilience evidence, not just good intentions





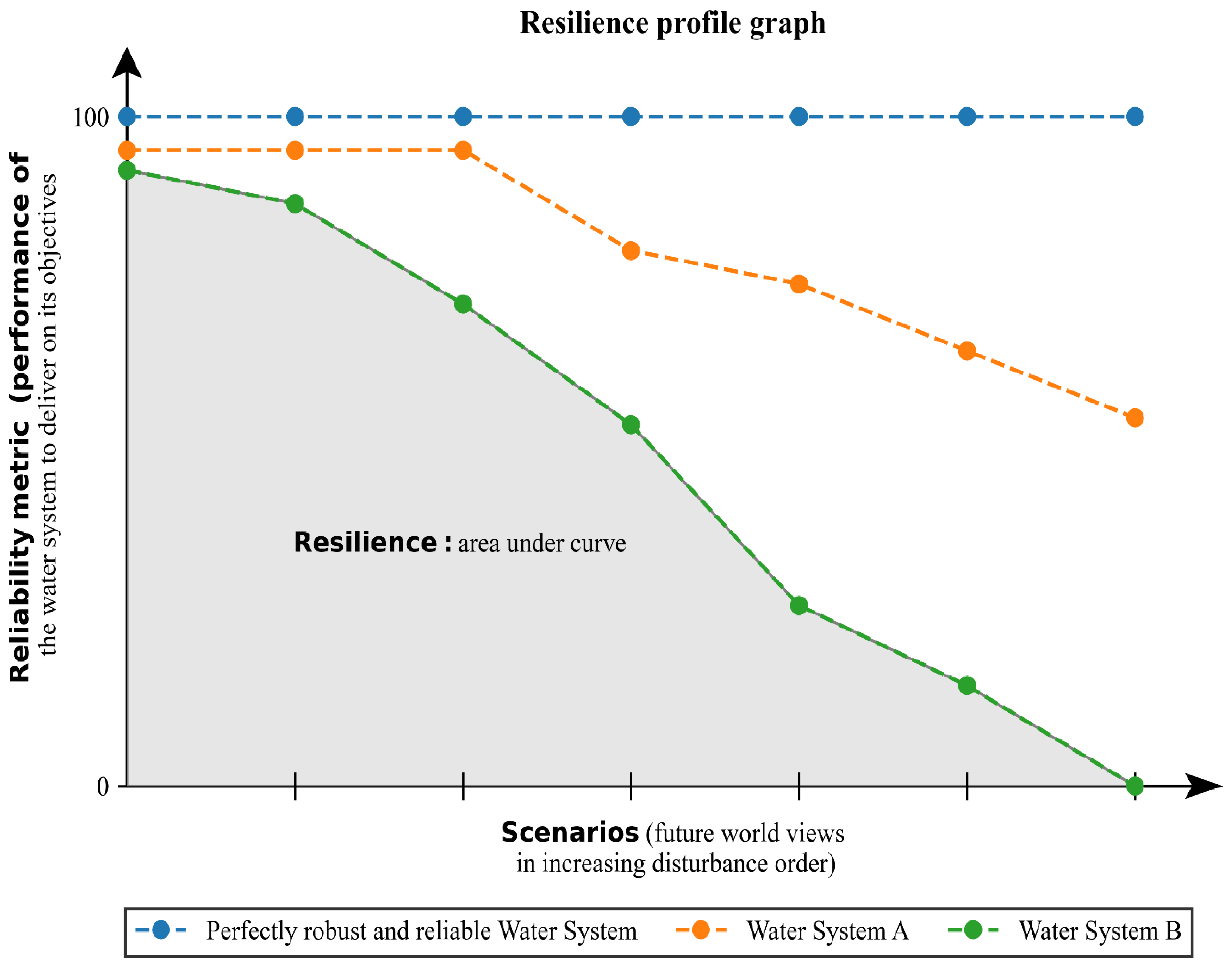
- New EU Directives: Moving from “best effort" to “auditable evidence”.
- Continuity obligations for critical entities are now being defined.
- There is a need for (as yet unspecified) forensic-level resilience metrics.

From reliability to safe-to-fail resilience

The idea is that we need to move from a design that aims (only) at reliability, i.e. the effort to build infrastructure that "must not fail" to designs in which (inevitable) failure is as "safe" as possible.

[fail-safe vs safe to fail]

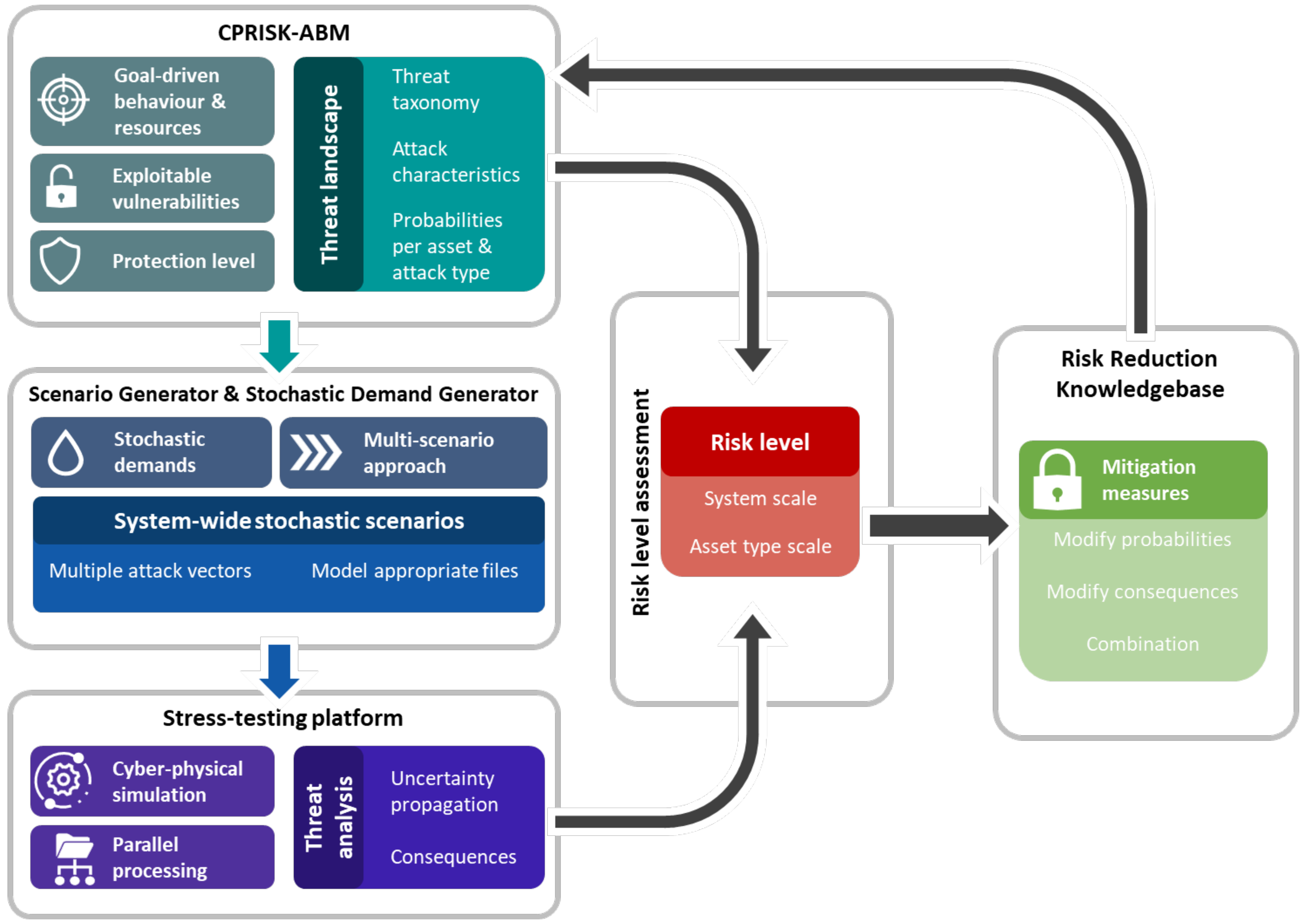
To see how the **system** "breaks" we must "push" it (by simulation) beyond the points of "normal operation".

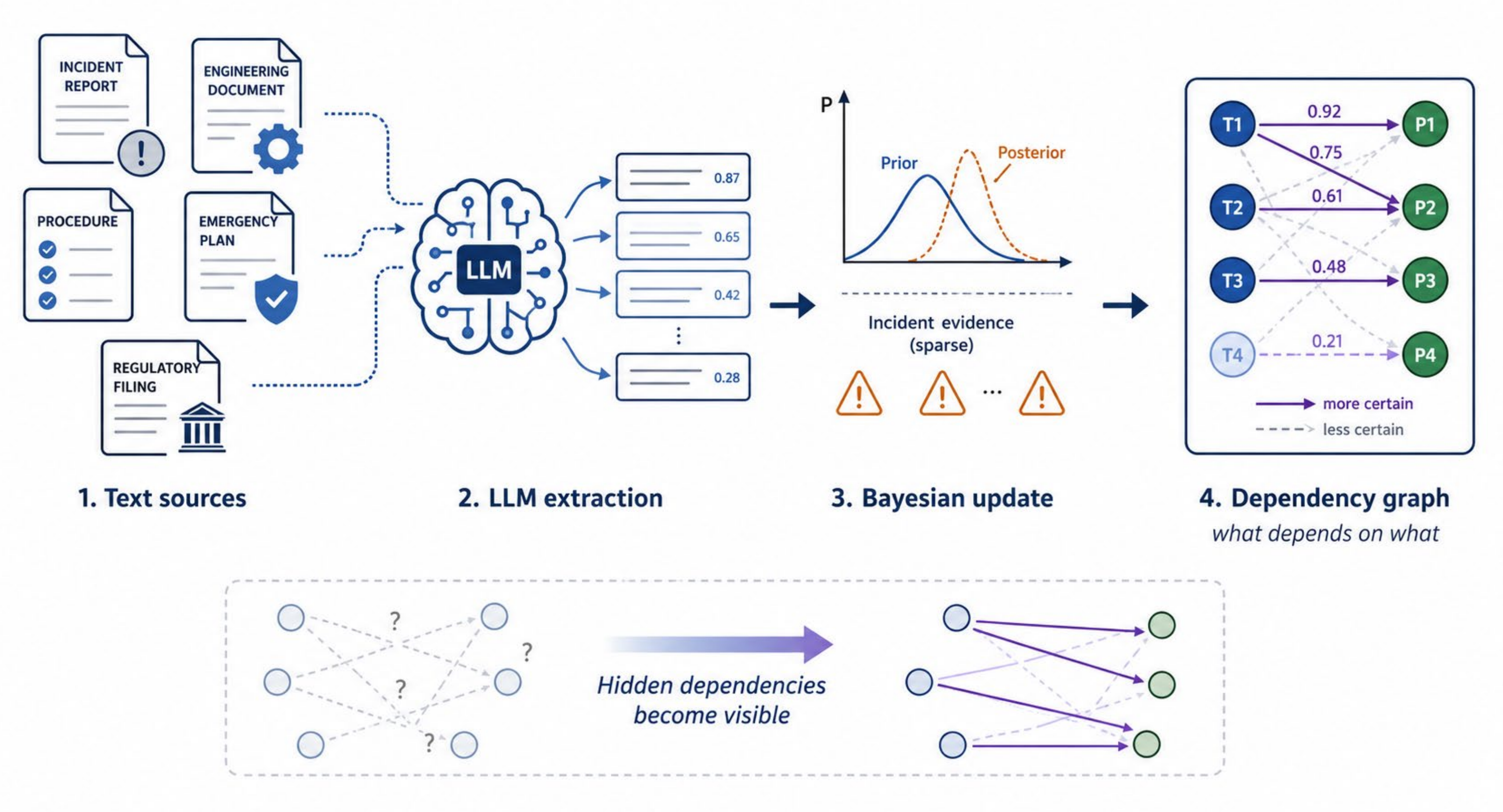


Makropoulos, C., D. Nikolopoulos, L. Palmen, S. Kools, A. Segrave, D. Vries, S. Koop, H.-J. van Alphen, E. Vonk, P. van Thienen, E. Rozos, and G. Medema. 2018. "A Resilience Assessment Method for Urban Water Systems." *Urban Water Journal* 15 (4): 316–328.

But then we have to ask: what is "the system"?

We tend to optimise our own systems, while critical dependencies sit *between* systems.



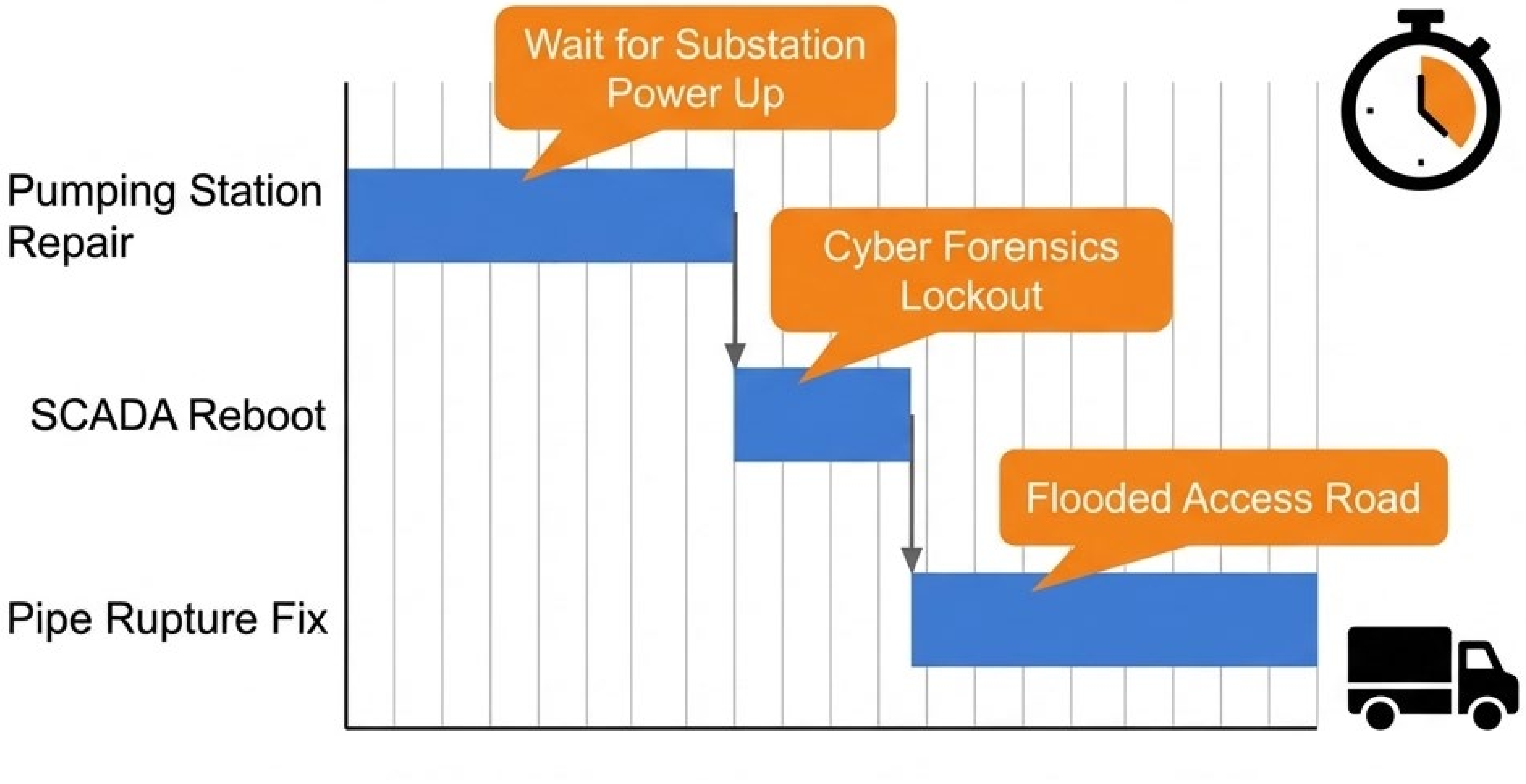


- Water infrastructure is **cyber-physical**: cyberattacks have physical effects (water quality, pressure) and the same successful attack can have different effects depending on control logic and hydraulic design.
- So, this is **not "just" an IT issue** - and we have not even begun to understand the vulnerabilities introduced by AI agents!

- We established that **infrastructures depend on each other**: the problem is that real risks often exist between them, not only within them.
- Identifying "**critical nodes**" of interdependence is difficult **technically** — and a nightmare **organisationally**.
- Who is **responsible** for **assessing** this — and **who pays**?

And there is also an elephant in the room: Recovery

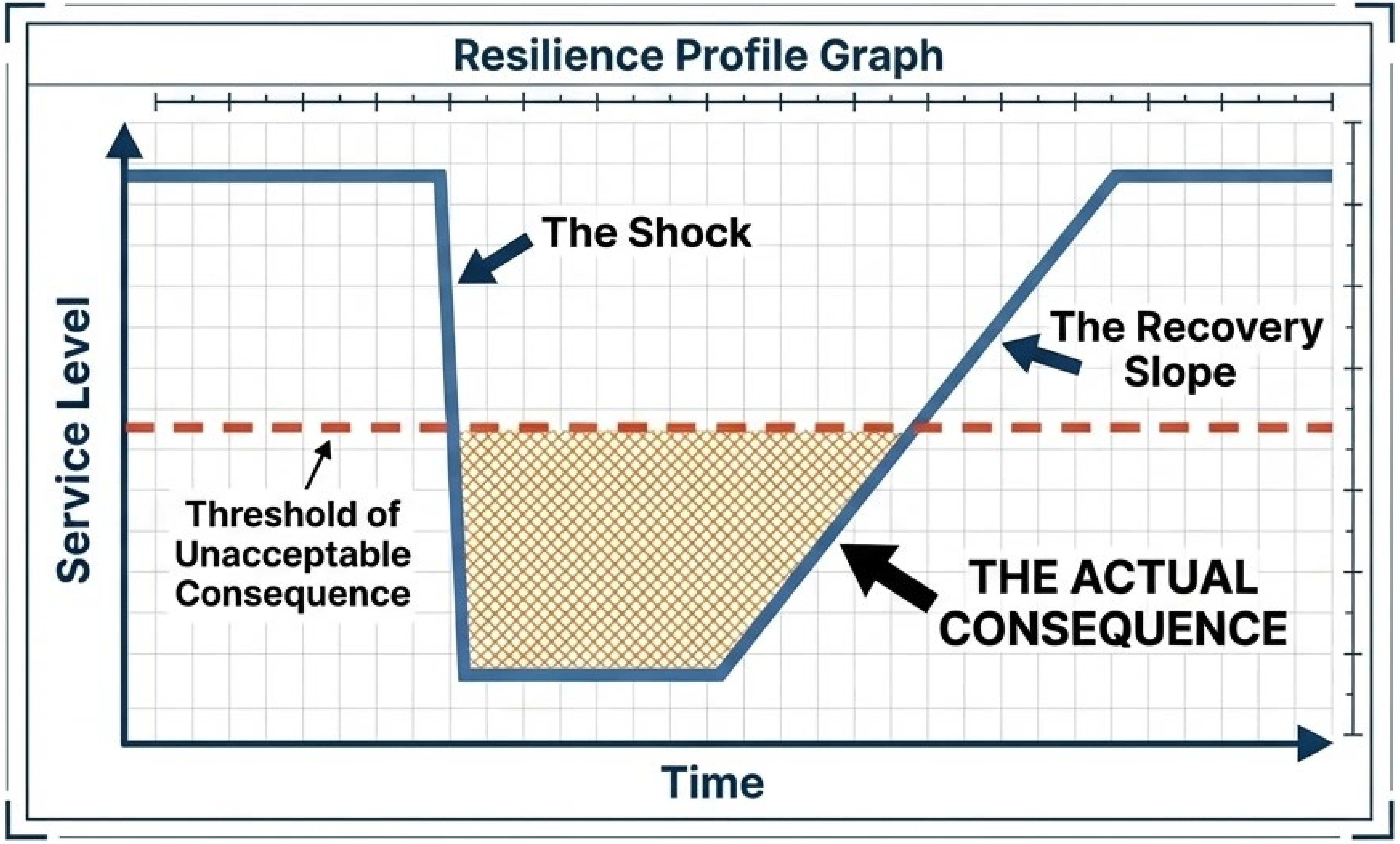
- Resilience must also be linked (**mathematically**) to the speed and quality of recovery.
- Recovery depends on personnel access, fuel for generators, repair times, and supply chains for critical components: **things that a water company does not control**.
- Recovery is a challenge of cross-sectoral coordination.



A recovery plan that does not account for fuel shortages, supply-chain disruption or traffic deadlocks due, for example, to a cyberattack on traffic lights, is wishful thinking …

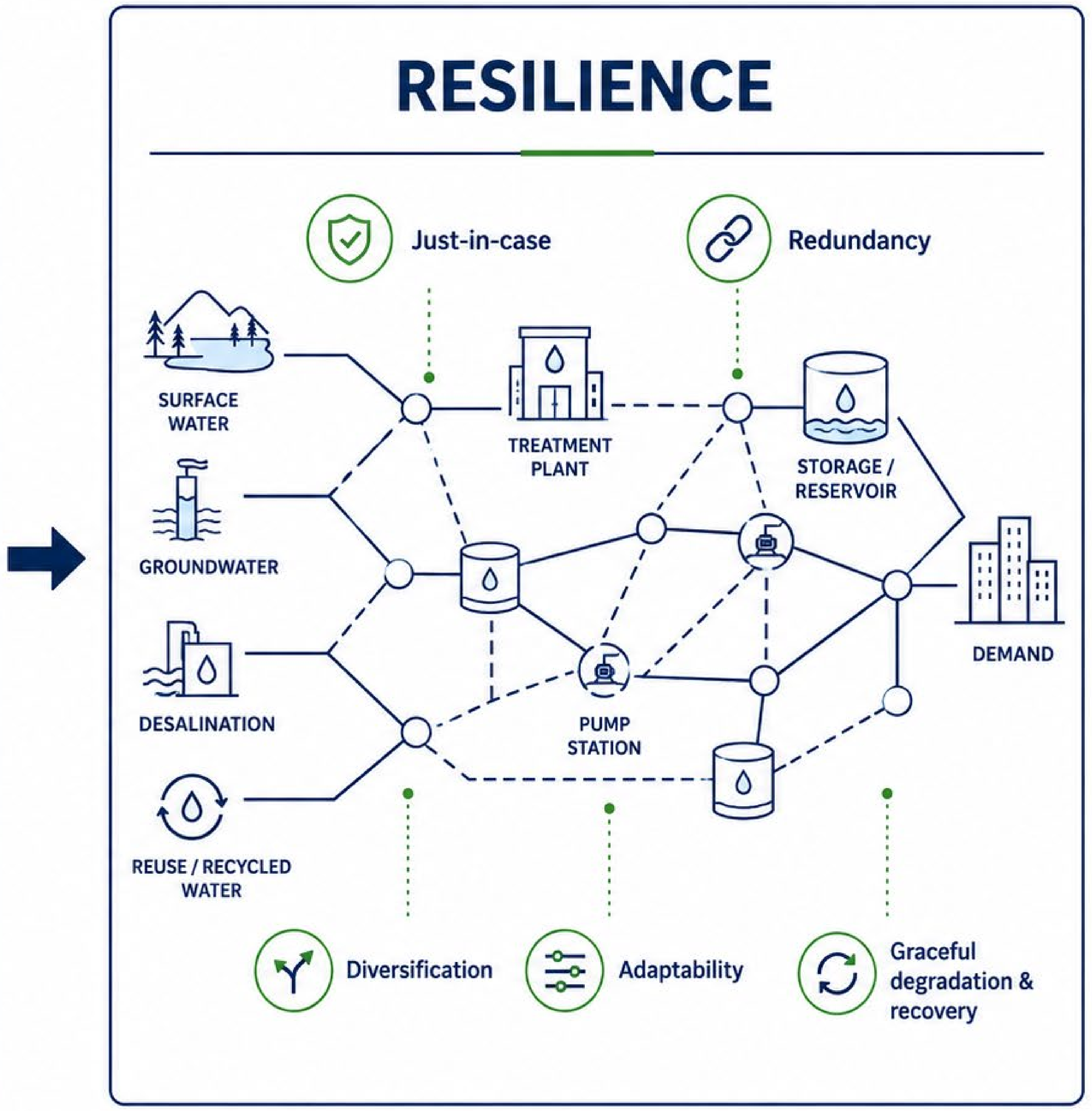
We should move from resilience profile assessments using these "stress tests" for infrastructure design

If we can't (**mathematically**) design the **resilience profiles** of our system (and those **interconnected** with it), including the **recovery curve**, we're not really protecting systems for the future: we're just hoping for the best.



But are we willing to pay for it?

- For decades we have focused on **optimisation** (of cost and performance under normal operating conditions).
- Resilience shifts our design objective functions to **redundancy,** back up systems, just-in-case options.
- **But these are not cheap:** do we understand what this shift implies in terms of investments required over the next decade or so (in money, time, effort, skills but mindset?)



So, what intelligence do we still need?

- **Decision-grade data:** From sensor streams, SCADA, EO, GIS, maintenance logs and field reports into trusted, continuous, quality-controlled evidence.
- **Cyber-physical integrity:** Monitoring and control strategies that assume data may fail, be delayed, corrupted, spoofed or maliciously manipulated.
- **Hybrid twins and bounded autonomy:** Digital twins, ML and AI agents that support operation, stress-testing and explanation — but remain physically constrained, auditable and compliant.
- **Uncertainty-aware resilience evidence:** Stress tests, resilience profiles, recovery curves and transparent uncertainty disclosure that support comparison across CIs.
- **Human judgement in an AI-mediated loop:** AI may help decision-makers understand complex interdependencies - but if its “too helpful”, it could bias the human oversight we rely on.

So, the key challenge is not whether CIs can become more intelligent – **but how we ensure that this additional intelligence can be trusted under stress.**

We are not starting from scratch – but there is much to do and very limited time…

- Makropoulos, C., D. Nikolopoulos, L. Palmen, S. Kools, A. Segrave, D. Vries, S. Koop, H.-J. van Alphen, E. Vonk, P. van Thienen, E. Rozos, and G. Medema. 2018. **A Resilience Assessment Method for Urban Water Systems**. *Urban Water Journal* 15 (4): 316–328.
- Tsiami, L. and Makropoulos, C., 2021. **Cyber-Physical attack detection in water distribution systems with temporal graph convolutional neural networks**. *Water*, *13*(9), p.1247.
- Nikolopoulos, D. and Makropoulos, C., 2022. **Stress-testing water distribution networks for cyber-physical attacks on water quality**. *Urban Water Journal*, *19*(3), pp.256-270.
- van Thienen, P., Chatzistefanou, G.A., Makropoulos, C. and Vamvakeridou-Lyroudia, L., 2023. **What water supply system research is needed in the face of a conceivable societal collapse**?. *Journal of Water and Climate Change*, 14(12), pp.4635-4641.
- Tsiami, L., C. Makropoulos, and D. Savic. 2025. **Rethinking Urban Water Network Design: A Reinforcement Learning Framework for Long-Term Flexible Planning**. *Water Resources Management* 39: 7155–7174

URBAN WATER MANAGEMENT AND HYDROINFORMATICS GROUP

ISSRI
Institute for Smart, Sustainable & Resilient Infrastructure

NATIONAL TECHNICAL UNIVERSITY OF ATHENS

Cyber-Physical Water Infrastructure under Climate Extremes and Human Threats

Christos Makropoulos

Professor, School of Civil Engineering

Director, Laboratory of Applied Hydraulics

Director, Institute of Smart, Sustainable and Resilient Infrastructure