Panel #4

LISBON
April 2026

Theme

Complex Systems and Protection of Critical Infrastructure

ComputationWorld 2026 & DataSys 2026

Speakers

LISBON
April 2026

Moderator

Prof. Dr. Malte Prieß, HAW Kiel - Faculty of Computer Science and Electrical Engineering, Germany

Panelists

Lect. & Adj. Prof. Dr. George R S Weir, University of Strathclyde, Glasgow, UK

Dr. Steve Chan, Decision Engineering Analysis Laboratory, USA

Chair Introduction

LISBON
April 2026

Dr. George Weir — Strathclyde, Glasgow & Adjunct Prof. at Simon Fraser University, Canada. Research in cybersecurity, digital forensics, and social engineering.
critical infrastructure is always a socio-technical system — human frailty and system complexity are inseparable.

Dr. Steve Chan — Decision Engineering Analysis Laboratory, USA. Harvard and MIT alumnus, 13 patents, 80+ publications including 37 IEEE papers. Former Chief Innovation Officer at a Fortune 500 company.
AI data centers want to monitor their own infrastructure with AI — but the technical hurdles are significantly underestimated.

Chair Introduction

LISBON
April 2026

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

My background is in Cloud Computing, AI, Data Science and Software Engineering.

MAX-PLANCK-INSTITUT FÜR GRAVITATIONSPHYSIK (ALBERT-EINSTEIN-INSTITUT)

Leibniz Universität Hannover

C A U Christian-Albrechts-Universität zu Kiel

d-fine

DH DUALE SH HOCHSCHULE SH

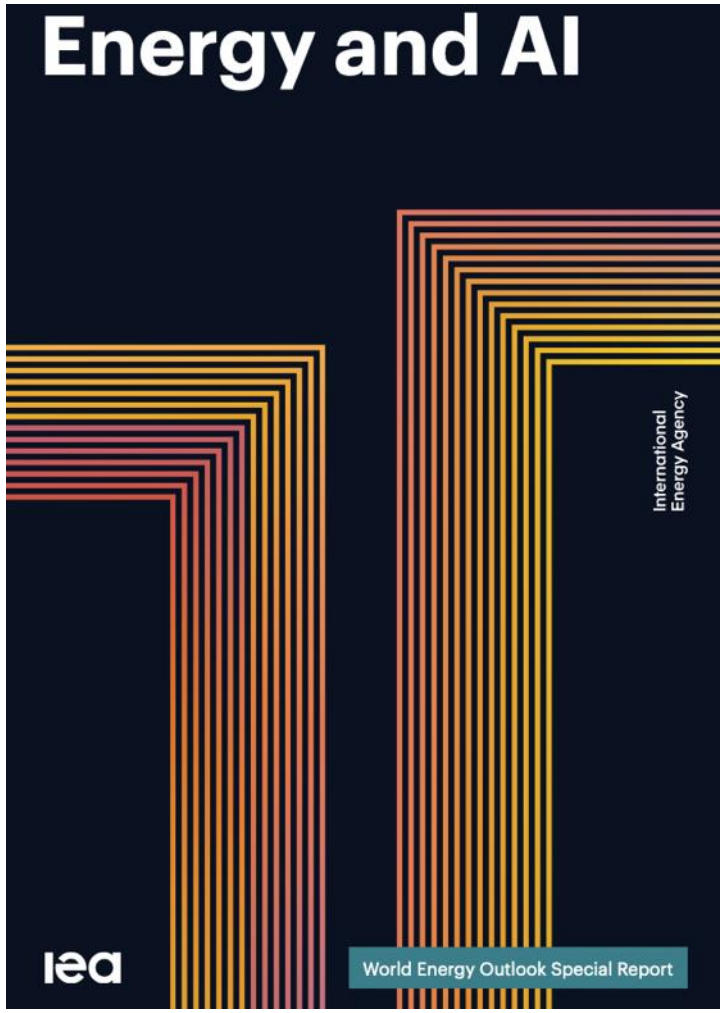
HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

My perspective: we should treat critical infrastructure protection like we treat building reliable distributed systems.

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?



Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

Chair Introduction

LISBON
April 2026

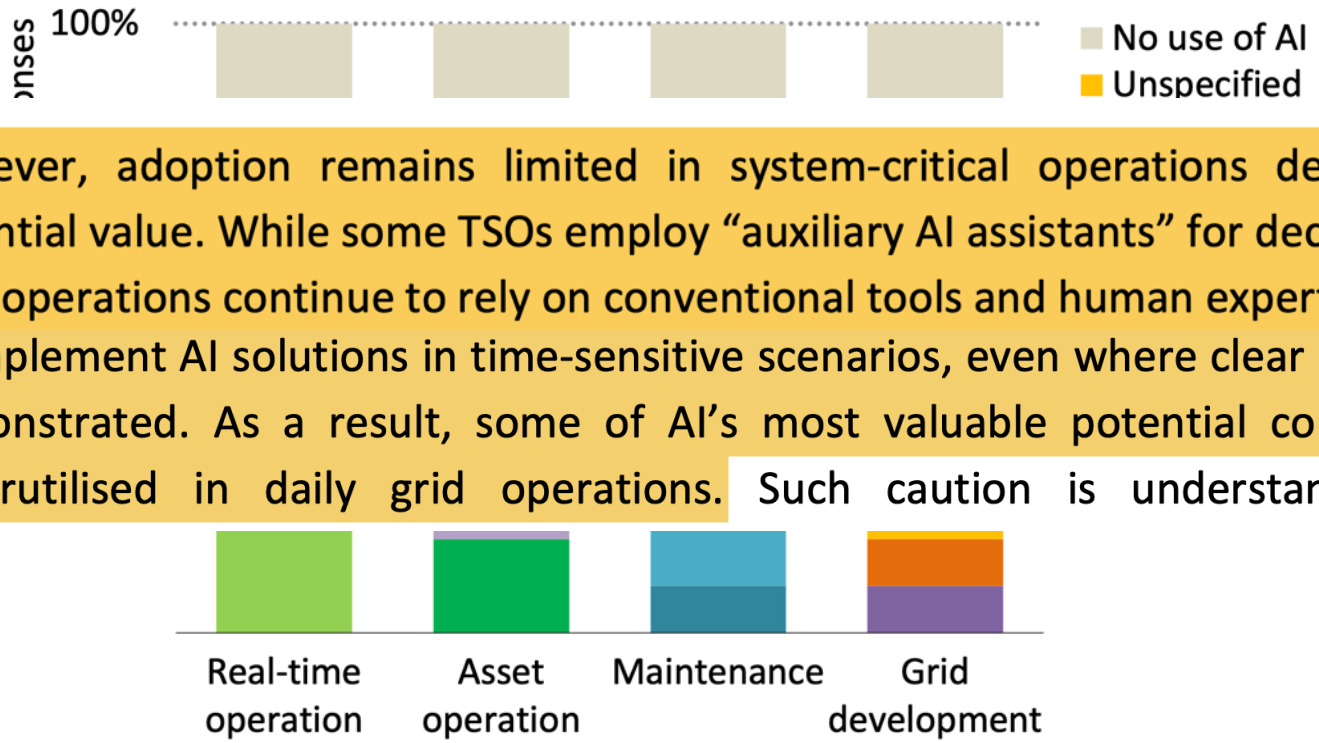
Setting the Stage — Why This Panel, Why Now?

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

Figure 3.7 ▷ **Utilities using AI applications by category, 2024**



However, adoption remains limited in system-critical operations despite their higher potential value. While some TSOs employ "auxiliary AI assistants" for decision support, real-time operations continue to rely on conventional tools and human expertise, with hesitancy to implement AI solutions in time-sensitive scenarios, even where clear benefits have been demonstrated. As a result, some of AI's most valuable potential contributions remain underutilised in daily grid operations. Such caution is understandable for critical

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?

Cybersecurity enhancements to protect critical infrastructure: As energy systems are becoming increasingly electrified, integrated and connected, their vulnerability to cyberattacks has also increased. AI-enabled cybersecurity features, such as enhanced threat detection and more responsive protection, can help secure energy systems. On the flip side, AI can also be used to make systems more vulnerable, as discussed in

by the presence of legacy information technology (IT) infrastructure, automation, cloud computing and reliance on third-party vendors that might not have secure systems (IEA, 2021a). Intrusions by malicious actors have exposed critical infrastructure to disruptions,

These episodes underscore the need for energy systems to become more resilient to cyberattacks. AI acts as a force multiplier in both directions, enhancing threat detection and enabling more responsive protection on the one hand while simultaneously empowering adversaries with tools for sophisticated attacks on the other. AI applications

Prof. Dr. Malte Prieß

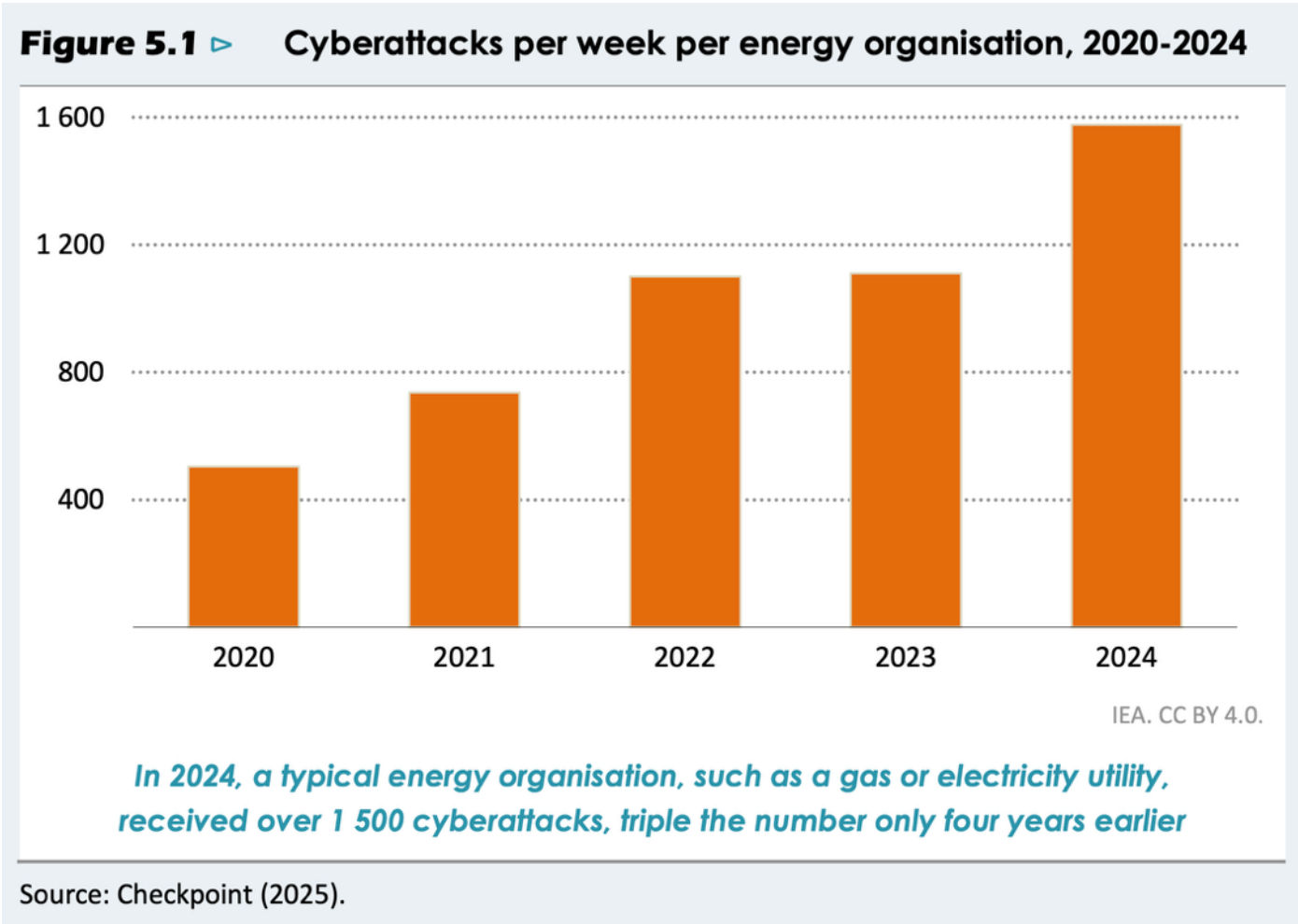
Professor for Cloud Technologies

HAW Kiel, Germany

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?



Prof. Dr. Malte Prieß

Professor for Cloud Technologies

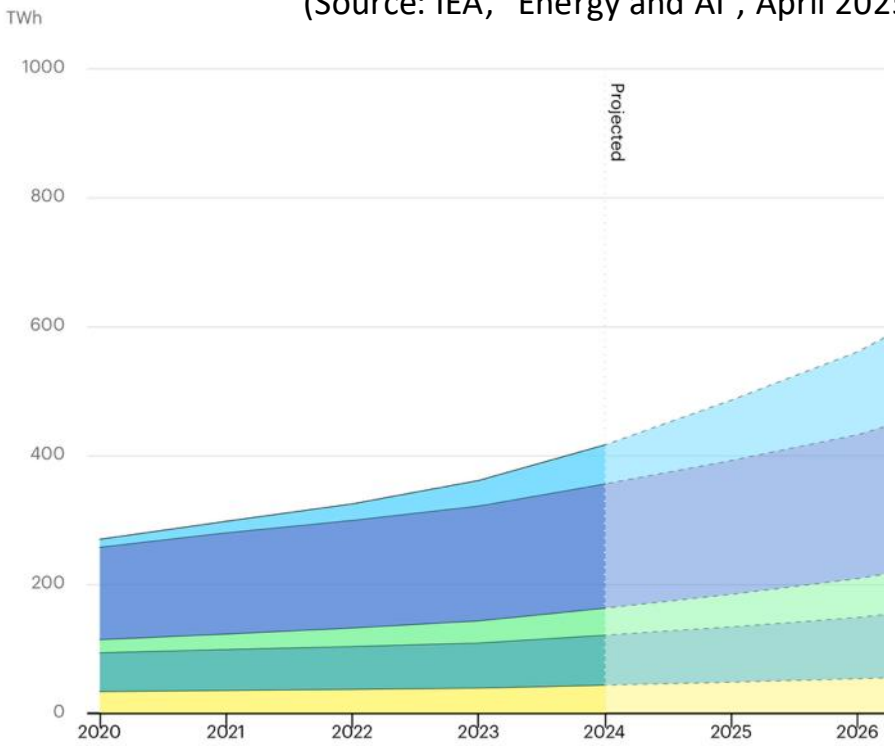
HAW Kiel, Germany

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?

Global data centre electricity consumption
(Source: IEA, "Energy and AI", April 2025, CC BY 4.0)



Accelerated servers Conventional servers Other IT equipment Cooling Other infrastructure

Prof. Dr. Malte Prieß

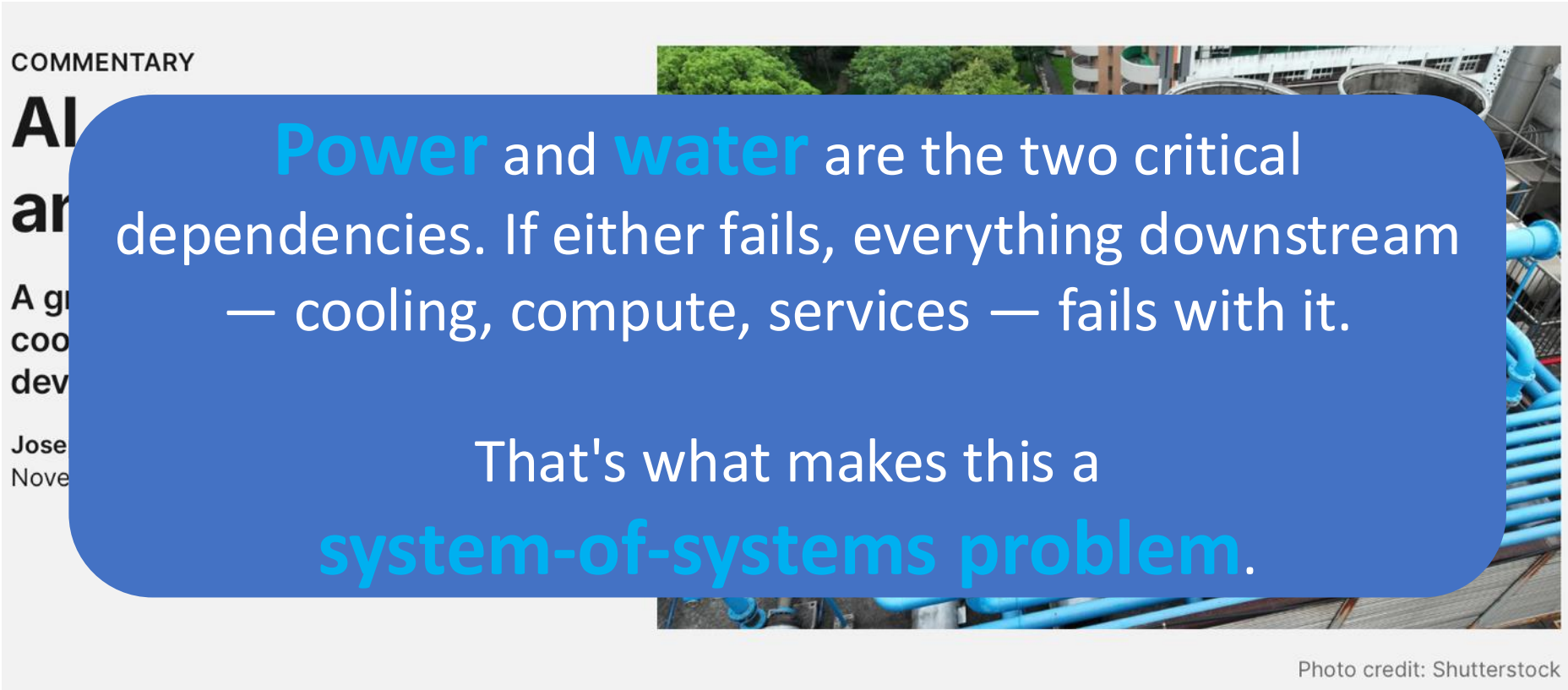
Professor for Cloud Technologies

HAW Kiel, Germany

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?



Power and **water** are the two critical dependencies. If either fails, everything downstream — cooling, compute, services — fails with it.

That's what makes this a **system-of-systems problem**.

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

Chair Introduction

LISBON
April 2026

Setting the Stage — Why This Panel, Why Now?

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

- **Complex, interconnected, fragile:** Our digital world depends on physical infrastructure that is growing more complex, more interconnected, and more fragile.
- **AI Data Centers (AIDC)** are a perfect case study: they are critical infrastructure that simultaneously depends on other critical infrastructure (power grids, water supply, telecom networks) and is becoming critical infrastructure for society at large.
- **Scale of the problem:** Data centers consumed ~415 TWh globally in 2024 (~1.5% of global electricity). By 2030, this is projected to double to 945 TWh — equivalent to Japan's total electricity demand (IEA, 2025). Large data centers can consume up to 5 million gallons of water per day (Brookings, 2025).
- **Not isolated systems:** They form a system-of-systems where failures in one domain (power, cooling, network) cascade into others. — a defining characteristic of complex systems.

Chair Introduction

LISBON
April 2026

The Key Tensions — What Makes This Hard?

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

- **The AI Protector Paradox:** We want to use AI for condition monitoring, anomaly detection, and self-healing — but the AI systems themselves are vulnerable (adversarial attacks, data poisoning, false positives/negatives). The protector needs protection.
- **Scale vs. Observability:** As systems grow in scale and density (thousands of sensors, extreme power densities, heterogeneous hardware), achieving reliable observability becomes exponentially harder. Silent errors (thermal throttling, gradual degradation of fans/pumps) may go undetected until cascading failure occurs.
- **The Training Data Dilemma:** AI-driven anomaly detection depends on training data. Generating realistic synthetic anomaly data ⇢ non-trivial AI problem.
- **Speed of Deployment vs. Maturity of Protection:** Hyperscalers are investing hundreds of billions of dollars annually in AI infrastructure — estimates range $330B to > $500B, but the condition monitoring and self-healing frameworks are still immature.

Chair Introduction

LISBON
April 2026

Panel Roadmap & Key Questions for Discussion

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

- **Self-Healing Systems — realistic or aspirational?** Can we genuinely build infrastructure that detects, diagnoses, and recovers from faults autonomously? What are the preconditions? What are the risks of automated response systems acting on false signals?
- **Cascading Failures:** How do we model and prevent failure propagation across tightly coupled subsystems (power ⇢ cooling ⇢ compute ⇢ services)? What role does resilience engineering play vs. traditional redundancy? (⇢ Google London DC outage 2022)
- **Trust in AI for Critical Infrastructure:** If the AI models monitoring critical infrastructure can themselves be compromised (deepfakes, data poisoning, adversarial inputs), how do we establish trustworthy monitoring pipelines? Who watches the watchmen?
- **Cyber-Physical Security:** As physical infrastructure becomes software-defined (smart grids, intelligent cooling), the attack surface expands. How do we secure the convergence?
- **The Human Factor:** Where should humans remain in the loop, and where is full automation both safe and necessary?

Panelist Position

LISBON
April 2026

Increasingly AI Data Centers (AIDC) are taking on the responsibility to monitor their own Strategic/Critical Infrastructure (SCI)

- AIDC have an extensive requirements for power, water, and other utilities. For example, a 100 MW AIDC (× 24 hours × 365 days) might require ≈ 876,000 MWh (876 GWh) of energy use, and just the on-site cooling might consume 1.2 million gallon of water per day for a 100MW AIDC and 5+ million gallons for a 500MW AIDC (Source: Control Associates Inc.)
- To alleviate the concern of potential power outages, water shortages, etc. in their host communities due to this massive consumption, AIDC are taking more responsibility for their SCI.

Dr. Steve Chan

Decision Engineering

Analysis Laboratory

Panelist Position

LISBON
April 2026

Protection of SCI includes Condition Monitoring (CM) and Early Fault Detection (EFD)

- Currently, many hyperscale AIDC keep track of their Power Usage Effectiveness (PUE) (e.g., electricity usage per rack, per server, Uninterruptible Power Supply or UPS status, etc.). In some cases, renewable energy is on-site, and this needs to be monitored as well. The AIDC also monitor for aisle temperatures, coolant flow, humidity performance, liquid cooling status (e.g., high-density GPU/TPU clusters for AI training/inference), etc
- Interestingly, some AIDC aim to contribute their AI capabilities to their own Condition Monitoring (CM) and Early Fault Detection (EFD), via AI-facilitated automated anomaly detection pipelines for CM/EFD. These AIDC are endeavoring to detect anomalies, predict failures before they happen, optimize efficiency (e.g., energy, water, etc.); for Information Technology (IT) infrastructure (e.g., communications), the utilized term regarding AI for IT Operations is AIOps. The AIDC are also endeavoring to deploy Automated Response Systems (ARS). The combination of CM/EFD with ARS form the backbone of an envisioned Self-Healing Infrastructure (SHI) paradigm.
- However, the desired robust CM/EFD for SHI turns out to be a non-trivial endeavor.

Dr. Steve Chan

Decision Engineering

Analysis Laboratory

Panelist Position

LISBON
April 2026

The Critical Need for CM and EFD

- **AIDC well recognize the criticality for CM/EFD**. The extreme power density, thermal management complexity, and myriad of sensors all constitute a worrisome load for AIDC Operations & Maintenance (O&M) efforts. The ongoing challenges include certain silent errors (e.g., thermal throttling/clock speed reduction when certain temperatures are reached, soft errors from electrical noise, etc.), natural degradation (e.g., of airflow fans for cooling, which can lead to thermal throttling; of pumps for circulating coolant in liquid-cooled racks, which can also lead to thermal throttling; of servers, which can lead to memory faults/incorrect computations), power quality issues (e.g., voltage surges/spikes, harmonics, transients), etc. Beyond these, there are the CM/EFD-related anomalies, such as for the power-related SCI; the production of a corpus of sample anomalies to be detected (for conducting the AI training) even for this turns out to be non-trivial.

Dr. Steve Chan

Decision Engineering

Analysis Laboratory

Panelist Position

LISBON
April 2026

The Critical Need for CM and EFD

- **The described challenge turns out to be quite difficult even under ideal conditions; unfortunately, ideal conditions are not commonplace**. Taking just one challenge - the generation of test images (containing sample anomalies to be detected) for conducting the AI model training - the associated technical challenges include, among others, training data bias, token interpretation variability, latent space sensitivity (i.e., how alterations in the compressed, lower-dimensional form of the original latent space affect the output of the involved AI model), etc. The complexities surrounding CM/EFD are starting to give AIDC pause regarding these O&M endeavors.

Dr. Steve Chan

Decision Engineering

Analysis Laboratory

Panelist Position

LISBON
April 2026

The Critical Need for CM and EFD

- **While Generative AI (GenAI) can indeed be leveraged for the creation of synthetic anomaly images/datasets for training the underpinning AI systems of the AIDC CM/EFD anomaly detection systems, there are a number of looming issues to consider.** For example, AI-facilitated automated anomaly detection pipelines are beset with a variety of potential upstream issues (e.g., deepfakes, false images, contrived information, etc.), and the ensuing downstream effects (e.g., False Positives or FPs, False Negatives or FNs) must be contended with. Since AI models train on massive (often uncurated) datasets, which are challenging to audit, various adversarial attack vectors, such as data poisoning, can profoundly impact the AI model training/updating.

Dr. Steve Chan

Decision Engineering

Analysis Laboratory

Panelist Position

LISBON
April 2026

- **My background** is in Human Computer interaction, AI, Internet of Things, and Cloud Security.
- **My perspective**:
  - We should treat critical infrastructure protection like we treat other safety-critical systems.
  - Such systems are never wholly isolated autonomous facilities.
  - People are key components in the design, commissioning, operation, and maintenance of critical systems.
  - Protection and other precautionary measures must consider and allow for the human element in the socio-technical system.

Dr George Weir

University of Strathclyde

Panelist Position

LISBON
April 2026

- **Two primary factors:**
  - Human frailty, and
  - System complexity
- **These factors intersect:**
  - Design flaws (slips and errors)
  - Unanticipated ‘features’
    - Functions of complexity
    - Emergence?
  - Misunderstandings
- **Bad actors**
  - Rely on the above factors
  - Misuse?
- **Remedy?**

Dr George Weir

University of Strathclyde

Panelist Position

LISBON
April 2026

- Remedy?
- Socio-technical system modelling and analysis
  - Scope for application of (defensive) AI
- Better training
- More sophisticated monitoring
- Awareness of human susceptibility to social engineering

Dr George Weir

University of Strathclyde

Panelist Position

LISBON
April 2026

Albladi and Weir *Cybersecurity* (2020) 3:7
https://doi.org/10.1186/s42400-020-00047-5

Cybersecurity

Dr George Weir

University of Strathclyde

RESEARCH Open Access

Predicting individuals' vulnerability to social engineering in social networks

Samar Muslah Albladi[1*] and George R. S. Weir[2]

Abstract

The popularity of social networking sites has attracted billions of users to engage and share their information on these networks. The vast amount of circulating data and information expose these networks to several security risks. Social engineering is one of the most common types of threat that may face social network users. Training and increasing users' awareness of such threats is essential for maintaining continuous and safe use of social networking services. Identifying the most vulnerable users in order to target them for these training programs is desirable for increasing the effectiveness of such programs. Few studies have investigated the effect of individuals' characteristics on predicting their vulnerability to social engineering in the context of social networks. To address this gap, the present study developed a novel model to predict user vulnerability based on several perspectives of user characteristics. The proposed model includes interactions between different social network-oriented factors such as level of involvement in the network, motivation to use the network, and competence in dealing with threats on the network. The results of this research indicate that most of the considered user characteristics are factors that influence user vulnerability either directly or indirectly. Furthermore, the present study provides evidence that individuals' characteristics can identify vulnerable users so that these risks can be considered when designing training and awareness programs.

Keywords: Deception, Information security, Phishing, Social engineering, Social network, Vulnerability

Panelist Position

LISBON
April 2026

A Cloud & AI Perspective on Infrastructure Resilience

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

- **From Cloud we already know:** Redundancy alone is not enough. We need observability, chaos engineering, graceful degradation, and well-defined failure domains. These principles translate directly to physical infrastructure protection.

- **Cloud practices for physical infrastructure:** The same practices that made cloud systems reliable — circuit breakers, health checks, automated failover, blast radius limitation — should be systematically applied to cyber-physical critical infrastructure.

- **But there is a gap:** Cloud software can be patched, rolled back, redeployed in seconds. Physical infrastructure (power transformers, cooling systems, water pipes) cannot. This asymmetry is underappreciated. Our models for resilience need to account for the irreversibility and time constants of physical systems.

Panelist Position

LISBON
April 2026

From AIOps to "AI for Infrastructure" — Opportunities and Risks

Prof. Dr. Malte Prieß

Professor for Cloud Technologies

HAW Kiel, Germany

- **AIOps is a starting point:** Using AI for IT operations monitoring is more established. Extending this to physical infrastructure monitoring (power, cooling, water) is challenging — but it raises the stakes dramatically ⇢ A false negative in IT means a degraded service. A false negative in power infrastructure can mean a blackout.
- **What's needed:**
  - Robust, auditable training data pipelines (⇢ Steve Chan)
  - Explainable AI for critical decisions
  - Layered defense: AI monitoring should complement
  - Standards and benchmarks for AI-driven condition monitoring
- **Self-healing infrastructure?** Are we building self-healing infrastructure, or are we building infrastructure that thinks it can heal itself?