Center for International AI Governance and Innovation (CIAGI)

Advancing Safe, Secure, and Trustworthy AI Adoption in Critical Infrastructure

INDUSTRY & EXECUTIVE BRIEF | 2026

AI is being deployed in systems that power electrical grids, manage water supplies, and control industrial operations—often without adequate governance, security validation, or resilience planning. ***CIAGI exists to change that.***

THE BUSINESS PROBLEM

AI Deployment Without Governance	AI is entering OT environments ahead of formal governance, risk assessment, or security validation.
Existing Frameworks Leave Gaps	NERC CIP, ISA/IEC 62443, and the NIST Cybersecurity Framework (NIST CSF) were not specifically designed to address AI governance and assurance risks in cyber-physical environments.
Regulatory Pressure Is Accelerating	In December 2025, CISA, Australia's ACSC, and partner agencies published joint principles for the secure integration of AI in operational technology. Governance, assurance, safety, and security expectations are developing rapidly.
The Skills Gap Is Critical	The estimated global cybersecurity workforce gap reached 4.8 million professionals in 2024 (ISC2). Organizations also face a shortage of interdisciplinary expertise spanning AI governance, cybersecurity, and operational technology.

★ AAIGF-E — A PUBLISHED AI GOVERNANCE FRAMEWORK FOR THE ELECTRIC SECTOR

AAIGF-E v1.0 (Adaptive AI Governance Framework for the Electric Sector) is a published governance framework designed for the use of AI in electric-utility and associated OT environments. It was co-authored by **Suhail Ahmad Rana** and **Clint Bodungen**. Publicly available with attribution to the authors.

- 111 governance controls across 11 domains
- Mapped to NERC CIP, the NIST AI RMF, MITRE ATLAS, ISA/IEC 62443, and ISO/IEC 42001
- AAIGF-E v2.0 is in development, with broader sector applicability under consideration

The framework is supported by related research presented at international IEEE conferences and informed by engagement with standards and industry communities.

WHAT CIAGI OFFERS

- AI Governance Assessment — a structured gap assessment against the framework's 111 controls
- Pilot Validation — validate AI governance controls and operational workflows in the CPAG Lab before operational deployment
- AI Risk Scenarios — scenario-based exercises reflecting AI risks in OT and critical infrastructure environments
- Expert Advisory — specialist advisory support grounded in experience across critical infrastructure cybersecurity, governance, risk, and AI assurance

4.8M — Estimated global cybersecurity workforce gap (ISC2, 2024)

111 — AAIGF-E governance controls across 11 domains

HOW WE WORK | CPAG LAB — CYBER-PHYSICAL AI GOVERNANCE LABORATORY

CIAGI DELIVERY MODEL

RESEARCH
Evidence-based framework development

↓

AAIGF-E FRAMEWORK
111 controls across 11 domains

↓

ASSESSMENT TOOLKIT
Structured AI environment assessment

↓

PILOT VALIDATION
CPAG Lab validation before deployment

↓

GOVERN & SCALE
Platform • Sandbox • Training • Future Leaders

CPAG Lab

Cyber-Physical AI Governance Laboratory

WHAT IT IS

CPAG Lab is CIAGI's applied research and validation laboratory for AI governance in critical infrastructure. It bridges AI governance frameworks with operational environments by validating governance controls, assurance mechanisms, and human oversight before operational deployment.

PURPOSE

Transform AI governance from documented controls into operational evidence through practical validation, experimentation, and pilot studies.

CORE FUNCTIONS

- Validate AI governance controls
- Test AI assurance and human oversight
- Conduct OT/ICS cybersecurity experimentation
- Support pilot validation in operational environments
- Deliver executive demonstrations and stakeholder workshops
- Develop affordable modular laboratory kits for academia and industry

HOW CPAG LAB SUPPORTS AAIGF-E

CPAG Lab brings AAIGF-E into practice by validating, demonstrating, and continuously refining governance controls through experimentation, operational evidence, and pilot studies before deployment in critical infrastructure environments.

CURRENT STATUS

- AAIGF-E v1.0 published and publicly available
- CPAG Lab architecture and pilot capability under phased development
- Pilot partner discussions underway
- International research collaborations active
- AAIGF-E v2.0 in development

LEADERSHIP

Suhail Ahmad Rana

Founder & Executive Director

More than 18 years of experience in cybersecurity governance, risk, compliance, and AI governance across critical infrastructure environments. Co-author of AAIGF-E v1.0. Led cybersecurity governance activities for a national smart city critical infrastructure program in Saudi Arabia.

IEEE Senior Member | ISA Senior Member | CISA | CISM | CRISC | AAIA | AAISM | ISO/IEC 27001 Lead Auditor | ISO/IEC 42001 Lead Implementer

Dr. Dinara Kozhamzharova

Co-Founder & Academic Lead

Academic researcher specializing in artificial intelligence, the Internet of Things, smart infrastructure, and intelligent systems. Leads CIAGI's academic research and international research collaborations.

STRATEGIC ADVISORS

Prof. Eric T. Matson

Professor, Purdue University, USA

Strategic Advisor

- Artificial intelligence
- Multiagent systems
- Robotics and autonomous systems

Prof. Seunghwan Myeong

Professor, Department of Public Administration
Inha University, South Korea

Strategic Advisor

- AI governance
- Public policy
- Smart cities

BECOME A PARTNER

Become a Pilot Partner
Evaluate your AI governance posture using AAIGF-E and identify priority improvements before wider operational adoption.

Join the Early Adopter Program
Help shape AAIGF-E v2.0 through operational context and structured real-world feedback.

Commission an AI Governance Assessment
Structured assessment of AI use cases and governance arrangements against AAIGF-E's 111 controls.

Partner with CIAGI to advance safe, secure, and trustworthy AI adoption across critical infrastructure. ciagi.org | contact@ciagi.org | Suhail Ahmad Rana, Founder & Executive Director