
## Resilient Systems

Decentralised Security for Smart Cities and Critical Infrastructure

PROGRAM BRIEF

# FDP Quick Brief

Program Sponsors

Prepared for institutional planning, program evaluation, and strategic conversations with ATRISI.

hello@atrisi.org | atrisi.org

# Resilient Systems

### Decentralised Security & Infrastructure Intelligence

**Faculty / Professional Development Program**

## About the Program

Modern infrastructure is no longer protected by a single perimeter. Smart cities, campuses, utilities, transport systems, and critical infrastructure operate across distributed assets, vendor systems, IoT devices, OT networks, cloud platforms, and human decision layers.

Traditional NOC/SOC models are evolving into federated intelligence systems where security, operations, resilience, and governance must work together.

**"Resilient Systems"** is designed as an enablement program to help institutions, faculty, professionals, and infrastructure leaders understand and design secure, decentralised, and intelligence-driven systems for modern infrastructure.

## Program Objectives

By the end of this program, participants will be able to:

- Understand the evolution from NOC/SOC to federated infrastructure intelligence
- Differentiate between IT security, OT security, cyber-physical systems, and resilience
- Map distributed infrastructure assets across smart cities, campuses, and utilities
- Apply zero trust, segmentation, and decentralised enforcement principles
- Design resilience workflows for cyber, physical, and environmental risks
- Use AI and data intelligence for predictive infrastructure risk management
- Build governance thinking for secure and resilient infrastructure ecosystems

## Program Structure

The program is structured across four progressive levels:

## Level 1: Resilience Sensemaking

- What is a resilient system?
- From cybersecurity to systemic resilience
- NOC, SOC, XOC, and infrastructure intelligence
- Why centralised security breaks in distributed infrastructure
- Introduction to IT, OT, IoT, edge, and cyber-physical systems

## Level 2: Decentralised Security Architecture

- Centralised vs decentralised vs federated models
- Zero trust for distributed infrastructure
- Identity, policy, access, and segmentation
- Edge enforcement and local autonomy
- Designing secure zones for smart cities, campuses, and utilities

## Level 3: Infrastructure Intelligence

- Turning fragmented signals into operational intelligence
- Asset mapping and topology thinking
- Satellite, sensor, CCTV, GIS, weather, and telemetry data
- Predictive risk models for infrastructure failure
- Example module: vegetation risk intelligence for power infrastructure

## Level 4: Governance, Simulation & Action

- Incident response and resilience workflows
- Cyber + OT + physical risk coordination
- Policy, compliance, and institutional readiness
- Simulation exercises for smart city / campus scenarios
- Designing a federated intelligence layer for infrastructure

## Key Outcomes

Participants will leave with:

- Smart city / campus infrastructure security architecture template
- IT/OT asset mapping framework
- Decentralised security zone design
- Resilience risk scoring model
- Incident response and escalation workflow
- Governance checklist for critical infrastructure resilience
- Optional prototype concept using JoaLLM as an intelligence layer

## Flagship Use Case Module

### Vegetation Risk Intelligence for Critical Infrastructure

This module demonstrates how satellite imagery, GIS data, weather signals, and power infrastructure maps can be combined to predict risk before failure occurs.

Participants learn how vegetation near power lines can become an infrastructure risk signal and how AI-enabled workflows can convert it into preventive action.

**Core idea:**

> Vegetation is not just an environmental issue.
> It is an infrastructure risk signal.

## Program Highlights

- Covers cyber, OT, physical, and environmental resilience
- Moves beyond traditional SOC/NOC thinking
- Designed around real infrastructure scenarios
- Includes smart city, campus, utility, and critical infrastructure examples
- Focuses on architecture, governance, and implementation readiness
- Can be delivered as FDP, professional workshop, or institutional enablement program

## Target Audience

- Faculty members in computer science, cybersecurity, civil engineering, electrical engineering, urban planning, and management
- Research scholars and PhD candidates
- IT and cybersecurity professionals
- Infrastructure and facility management teams
- Smart city and public sector administrators
- Utility, energy, transport, and campus operations leaders

## Duration & Format

The program can be delivered in flexible formats:

- **1-Day Intensive Program** — 6–8 hours
- **2-Day Workshop** — 12–16 hours
- **Extended Program** — 2–4 weeks with assignments and project outputs

Mode:

- On-campus / in-person
- Virtual
- Hybrid

## Certification

Participants receive a Certificate of Completion upon fulfilling participation requirements.

- Certificate issued by: **[Institution Name]**
- Co-branded optional: **ATRISI / JoaLLM / Partner Institution**

## Alignment with Quality Frameworks

This program aligns with:

- Cybersecurity and resilience capacity building
- Infrastructure safety and risk management
- Research and innovation in smart systems
- Governance and institutional preparedness
- Sustainable and resilient infrastructure goals
- Industry-academia collaboration in applied technology

## About the Facilitator

**Aeishwary Mishra**
Principal Cloud Architect at Oracle

- Experience across enterprise cloud, cybersecurity, AI systems, and digital transformation
- Former academic leadership role in Computer Science
- Founder of ATRISI — Applied Technology Research Institute for Societal Impact
- Building JoaLLM — a unified intelligence platform bridging knowledge, reasoning, and execution

## Closing Note

> "Resilience is not built by reacting to failures.
> It is built by sensing weak signals, federating intelligence, and acting before disruption occurs."