



IEEE Tunisia Section
Cybersecurity Local Group



IEEE
COMPUTER
SOCIETY
ISIMA Student Branch

IEEE COMPUTER SOCIETY ISIMA STUDENT BRANCH
UNMASKING CYBER THREATS V2.0

TECHNICAL CHALLENGE DOCUMENTATION

IEEE “SMARTSECUREGRID” CHALLENGE 2026

AI & Cybersecurity Innovation for Sustainable and Resilient
Energy Systems

Focus Domain: Energy Sector (AI + Cyber)

Date: 26/27 September

Location: Al Kasr hotel, Sousse



IEEE “SMARTSECUREGRID” CHALLENGE 2026

AI & CYBERSECURITY INNOVATION FOR SUSTAINABLE AND RESILIENT ENERGY SYSTEMS

CALL FOR INNOVATION

The IEEE SmartSecureGrid Challenge 2026 invites students, researchers, innovators and startups to create transformative solutions combining Artificial Intelligence and Cybersecurity to secure and optimize modern power systems.

The global transition toward renewable energy sources such as photovoltaic solar systems, wind farms, hydroelectric generation, microgrids, battery energy storage systems (BESS), and distributed energy resources (DERs) is transforming the electrical power sector.

While these technologies significantly improve sustainability, they also introduce several critical challenges:

- Intermittent and unpredictable energy production
- Increasing complexity of energy distribution networks
- Risk of power overloads and cascading failures
- Vulnerabilities to cyberattacks targeting critical infrastructure
- Demand forecasting challenges
- Integration of millions of connected IoT devices and smart meters
- Need for autonomous decision-making and real-time optimization

Artificial Intelligence offers unprecedented capabilities for prediction, optimization, anomaly detection, and automation. However, AI systems themselves require robust cybersecurity mechanisms to ensure trustworthiness, resilience, privacy, and operational continuity.

The future of energy systems will depend on the convergence of:

- Artificial Intelligence (AI)
- Cybersecurity
- Smart Grids
- Renewable Energy Technologies
- Edge Computing
- Digital Twins
- Internet of Things (IoT)
- Advanced Analytics

This challenge aims to inspire students, researchers, innovators, and startups to develop groundbreaking solutions at the intersection of these strategic domains.



1. ABOUT THE CHALLENGE

The energy sector is rapidly evolving toward renewable generation, smart grids, distributed energy resources, connected devices and autonomous operations. This transition creates opportunities for AI-driven optimization but also expands the cyberattack surface of critical infrastructures.

The global energy sector is undergoing a major transformation. The integration of renewable energy sources such as photovoltaic solar systems, wind farms, hydropower, battery energy storage systems, smart grids, electric vehicles, and distributed energy resources is creating unprecedented opportunities for sustainable development.

However, this transformation also introduces significant challenges:

- Fluctuating renewable energy production
- Grid instability and load balancing issues
- Increasing energy demand
- Risk of cascading failures and blackouts
- Exposure to sophisticated cyberattacks targeting critical infrastructures
- Massive volumes of operational data requiring intelligent analysis

Artificial Intelligence (AI) has emerged as a key enabler for predictive analytics, energy optimization, anomaly detection, and autonomous decision-making.

At the same time, Cybersecurity has become a strategic pillar for protecting energy infrastructures against cyber threats, ransomware, malicious control commands, data manipulation, and attacks on Industrial Control Systems (ICS), SCADA, IoT, and smart-grid environments.

This challenge invites students, researchers, startups, and innovators to develop disruptive solutions that combine AI and Cybersecurity to create the next generation of secure, intelligent, and resilient energy systems.

2. CHALLENGE THEME

Securing and Optimizing the Future of Energy through Artificial Intelligence and Cybersecurity.

3. CHALLENGE OBJECTIVE

Develop and demonstrate an innovative Proof of Concept that leverages both AI and Cybersecurity to improve electricity generation, distribution, storage, resilience and operational security.

Participants must design and implement an innovative Proof of Concept (PoC) that leverages:

AI and CyberSecurity to improve one or more aspects of:

- Renewable energy production
- Smart-grid management
- Energy distribution
- Power quality
- Demand-side management
- Energy consumption optimization

- Blackout prevention
- Grid resilience
- Critical infrastructure protection

4. AI + CYBERSECURITY CONVERGENCE

Design an innovative AI-powered cybersecurity solution capable of predicting, protecting and optimizing energy infrastructures. Example topics include AI-powered cyberattack detection, autonomous cyber defense, digital twins for energy resilience, federated learning, cyber-physical attack prediction and intelligent blackout prevention.

Examples:

- AI detecting cyberattacks targeting renewable plants
- AI securing EV charging infrastructure
- Autonomous cyber defense for smart grids
- AI-powered microgrid resilience
- Federated Learning for secure energy analytics
- Cyberattack prediction impacting power generation or distribution

5. GRAND CHALLENGE STATEMENT

Predict. Protect. Optimize. Build a platform capable of forecasting energy generation and demand, detecting cyber threats, optimizing generation and distribution decisions, and preventing large-scale outages.

6. INNOVATION EXPECTATIONS

Projects will be evaluated on innovation, practicality, measurable impact, scalability, sustainability and technical excellence.

The proposed solution should demonstrate measurable impact in at least one of the following dimensions:

Energy Efficiency

- Reduced losses
- Better load balancing
- Improved renewable integration

Reliability

- Reduced outages
- Improved grid resilience
- Reduced blackout risks

Sustainability

- Increased use of renewable energy

Security

- Improved attack detection
- Reduced cyber risks
- Increased resilience of critical infrastructures

Innovation

- Novel AI techniques
- Emerging cybersecurity methods
- New business or operational models

- Carbon footprint reduction

7. DELIVERABLES

MAX 3 PAGES

EXECUTIVE SUMMARY

Including: Problem statement, Proposed innovation, Expected impact, Technology stack, Target users

MAX 15 PAGES

TECHNICAL REPORT

Covering: Background and literature review, System architecture, AI methodology, Cybersecurity architecture, Data sources, Risk analysis, Expected benefits, Scalability considerations

CORE REQUIREMENT

WORKING POC

The PoC must demonstrate the feasibility of the solution.

Accepted forms: Functional prototype, Software application, Digital Twin, Dashboard, Simulation platform, AI model, Hardware prototype, IoT demonstration

MAX 10 slides

PITCH DECK

Must include: Problem, Solution, Innovation, Architecture, Demonstration, Results, Impact, Business model (optional), Future roadmap, Conclusion

MAX 5 MINUTES

DEMONSTRATION VIDEO

The video should present: The challenge addressed, The proposed solution, Key innovations, PoC demonstration, Results obtained

8. COMPETITION PROCESS

Phase 1: Technical evaluation

Phase 2: Congress presentation consisting of a 10-minute pitch, 5-minute demonstration and 5-minute Q&A

note: everything must be submitted by the 24th of september or competitor team will be eliminated

9. EVALUATION AND SCORING CRITERIA

CRITERION	DESCRIPTION	SCORE
Innovation & Originality	Novelty and uniqueness	20
AI Excellence	Quality of AI approach	15
Cybersecurity Excellence	Security robustness	15
Energy Impact	Optimization benefits	15
Technical Feasibility	Implementation potential	10
PoC Quality	Maturity of prototype	10
Scalability & Sustainability	Long-term value	5
Business & Societal Impact	Economic/environmental value	5
Presentation & Communication	Pitch quality	5

10. INNOVATION BONUS POINTS

Real utility data (+2), Digital Twin (+2), Federated Learning (+2), Explainable AI (+2), Live cyberattack demonstration (+2). Maximum bonus: +10 points.

11. RECOMMENDED TECHNOLOGIES

AI:	Machine Learning, Deep Learning, Generative AI, Agentic AI, XAI, Federated Learning.
Cybersecurity:	SIEM, SOAR, IDS/IPS, Zero Trust, Threat Intelligence.
Energy:	Smart Grids, Microgrids, SCADA, AMI, Renewable Generation, BESS, EV Infrastructure.

12. GRAND CHALLENGE VISION

The jury will particularly value projects addressing the following grand challenge:

"Predict – Protect – Optimize"

Design an intelligent platform capable of:

- Predicting renewable energy production and energy demand using AI.
- Detecting and mitigating cybersecurity threats targeting critical energy infrastructures.
- Optimizing power generation, storage, and distribution in real time.
- Preventing overload conditions and reducing blackout risks.
- Improving resilience of future smart grids.

13. EXPECTED IMPACT

The challenge aims to stimulate the development of innovations that contribute to:

- United Nations Sustainable Development Goal (SDG) 7: Affordable and Clean Energy
- SDG 9: Industry, Innovation and Infrastructure
- SDG 11: Sustainable Cities and Communities
- SDG 13: Climate Action

while strengthening the cybersecurity resilience of critical power infrastructures worldwide.



UNMASKING CYBER THREATS V2.0

IEEE SMARTSECUREGRID CHALLENGE 2026

Organized by IEEE Computer Society ISIMA Student Branch
26–27 September 2026 | Tunisia