Call for Mission Mode Project Proposals – Oct 2024
(From Central/State Government funded Academic or Research Labs)

Foundation for Science Innovation and Development (FSID) at the Indian Institute of Science (IISc) and Power Grid Corporation of India Limited (PGCIL) have entered into a partnership to establish the "POWER GRID Center of Excellence (CoE) in Cybersecurity in Power Transmission and Grid Operation", to enable continuous R&D on cybersecurity program matching with the emerging requirements in the field of transmission and grid operation that would lay a strong foundation for achieving excellence in Cybersecurity of Operational Infrastructure. This facility would engage in R&D aspects of the cybersecurity of power systems.

Objectives:

1. To enable continuous R&D on cyber security programme matching with emerging requirements in the field of transmission and grid operation that would lay a strong foundation for achieving excellence in cyber security of Operational Infrastructure
2. To engage in R&D aspects of cyber security of power system including security analytics for situation awareness, competency building, development of defence systems for probable future cyber attacks
3. To act as a Center of Excellence and Think Tank for POWERGRID's cyber security concerns and to bring in experts from academia, research laboratories, and industry together under one umbrella to carry out cutting-edge research.

Deliverables:

1. Securing real-time connectivity between devices, sensors, and Operational Technology (OT) systems
    a) Assessment of security standards and recommendations
    b) Critical operators and assets Identification
2. Securing distributed and virtualized networks of Power System OT infrastructure.
    a) Field devices/protocols vulnerability assessment and creation of threat intelligence database
    b) Develop security risk assessment tools and risk mitigation techniques
    c) Evaluation of software-defined networking solutions
3. Capacity building
    a) Custom-designed courses in improving the competence of personnel in Transmission and Grid operations
    b) Imparting cutting-edge skills to handle a broad spectrum of conformance and auditing requirements

Broad Scope:

1. To recommend compliance mechanisms with the available specifications, standards, guidelines and to recommend a suitable policy and regulatory framework.
2. To recommend audit mechanisms to ensure conformance to suggested standards, guidelines, as well as facilitate development of audit capabilities.

3. To study issues of cyber security threat landscape in power transmission and grid operation.
4. To carry out asset mapping of critical infrastructure for cyber-physical dependency.
5. To develop and share a framework for testing of ~~the~~ systems including equipment to address supply chain security, detection solution and monitor malicious connections in Operational Technology (OT).
6. To carry out risk and vulnerability assessment of the communication infrastructure meant for monitoring, data acquisition and transfer, control, protection, automation etc. through AI/ML /big data analytics and identify mechanisms to address the issues, recommend mitigation to plug the gaps.
7. To provide capacity building, skill development, and design of cyber drills through training. Workshops/seminars for the personnel involved.
8. Methodology on Security analytics and event management - Forensic data analysis and anomaly detection.
9. Identify future cyber security challenges and provide mitigating measures.

PGCoE invites "Call for Mission Mode Project Proposals" to solve the problem statements mentioned below. The proposals are expected to have tangible outcomes in the form of usable software/hardware/appliances by POWERGRID utilities for testing the applicability in the field or in the realistic substation and control center testbed being created at PGCoE.

Eligibility

Central/State Government funded academic institutions & research labs.

Problem Statements

Sl No	Thematic Area	Problem Statement
P1	Secure Communication Protocols	Map IEC 61850-7-2 ACSI services to internationally standardized secure communication protocols. Focus deliverable to client/ server (Two party application association)
P2	Resilience to Denial-of-Service Attacks and ensure availability	Define mechanisms for legacy protection and control IEDs (Prior to 2015) to have resilience to DoS and DDoS attacks Focus the deliverable on the resilience of the IEDs to perform their intended function when communication port is under DoS.
P3	Cyber-Physical Security Convergence	Explore engineering grade solutions which would make certain utility automation process completely protected against cyber related threats Focus on target removal on at least one of the Mitre ICS attack patterns

P4	Security Configuration and Management	Develop a tools chain to increase detectability and visualize security. Asset management Focus on ICS based threat models.
P5	Incident Handling and Forensics	Design robust incident handling mechanisms to ensure, reliability, safety and continuity of business. Focus on restoration mechanisms, logging mechanisms for forensics
P6	Supply Chain Risk Mitigation	Explore and suggest robust mechanisms to handle supply chain risks Focus on development of test procedures to ensure leakages in supply chain are detected and identified before a component is used
P7	Predictive Intelligence	To generate possible future attack patterns / vectors that can possibly lead to a cyberattack.
P8	Trusted Models	Explore Trust based methodology for internal threat scenarios.
P9	Scenario Driven Cybersecurity training Simulator	To build a data driven / regenerative AI enabled cybersecurity training simulator. The simulator can use regenerative AI techniques to build attack and defence scenarios, providing an immersive and realistic experience and training.
P10	Security Monitoring	Data processing and Correlation, Situational awareness using AI learning models

Methodology

The problem/Input statement for design and development of tools, framework, the approach is as follows,

1. System/Software/User Requirements Specification document – T0 + 3months (T1)
2. Design & testing document - T1+ 3months (T2)
3. Development & module testing - T2+ 12 months (T3)
4. Integrated testing & User Manuals - T3+6 months

T-Start-date of the project

For more Information or clarification contact: Bapu S Bindhumadhava, Centre Head PGCoE bindhumadhav@fsid-iisc.in or office.pgcoe@fsid-iisc.in Phone 9844253414

Terms & Conditions

Submission Deadline

The last date for Submission of the proposal is 15th Nov 2024.

Minimum duration of the project is 24 months, and maximum duration is 36 months with total funding limited to 50 lakhs per project (including 10% overheads excluding GST). Proven existing solutions which require customization for power transmission and grid operations with shorter duration can also be considered based on the review committee recommendations. Proposals capital funds cannot be more than 20% of the total funding. Proposals requiring higher funding may be considered based on the project merits and deliverables. Any projects requiring higher capital should plan to use the existing infrastructure at PGCoE or should plan to augment infrastructure at PGCoE as much as possible.

Submission Link: **https://forms.gle/dvSKNK5UGZhLGRvT9**

Evaluation & Guidelines

1. Shortlisting will be based on the technical relevance to PGCoE scope and proposed outcomes.
2. Proposals should be only addressing cyber security of power transmission and grid operations. Outside this will not be considered for evaluations and no communication will be entertained on such proposals.
3. The proposals will be reviewed by a review committee of PGCoE.
4. Based on the committee recommendation shortlisted proposals will be called for presentations at PGCoE. No TA/DA will be provided.
5. The Final projects will be announced within 15 days after the presentations.
6. IP, copyright and know-how of the project outcomes will be as per the agreed upon terms between PGCoE and the beneficiary institute once the project gets approved.
7. Due acknowledgement must be made in any publications coming out of this funding including the project name and PGCoE. Combined acknowledgement with other funding agencies is not allowed.
8. Funds will be released every six months based on the review committee recommendations. Audited Utilizations Certificate to be provided annually.
9. Quarterly Progress Report to be submitted within a week after completion of the quarter.
10. Three project review meetings per year will be conducted for progress evaluation.

Project Proposal Template
PART A

Project Title:

Theme:

Duration:

Name and Affiliation of Principal Investigator	
Name and Affiliation of Co-Principal Investigators	

Executive Summary (1-page):

PART B – Technical Details

Please describe the project to make sure it contains the following sections.

- Problem statement and its relevance to the Theme
- Existing work of PI relevant to the theme
- Existing work of Co-PIs relevant to the theme
- Literature Review on the problem statement
- The research gaps are being addressed.
- Is the project an enhancement to existing work? YES/NO
  If YES clearly articulate what is already available and what will be done through this project
- The Technical Approach
- Tangible Outcomes
- Practical implementation and testing plan
- Milestones and timelines
- Measurable key performance indicators
- Training modules: (Some training modules for PGCIL employees are expected from faculty about 6 to 8 hours of lectures and associated practical sessions, to improve the cybersecurity capabilities)
- Appendix 1 - List of relevant publications of PI (last 3 years)
- Appendix 2 - List of relevant publications of Co-PIs (last 3 years)
- Appendix 3 – Investigator certificate
- Appendix 4 - Endorsement from Head of the Institution

PART B – Budget Details

SL.No	Year-I	Year-II
Manpower (1 Research staff (project assistant, research associate or postdoc, PhD/MTech(res) students)		
Minor Equipment (less than 2.5 lakhs)		
*Major Equipment		
Consumables & Contingency		
Travel (max 2L per year)		
Overheads (10%)		
GST (18%)		

*Please read the proposal evaluation process and guidelines

Appendix 3

Certificate from the Investigator (s)

Project Title:

1. I/We agree to abide by the terms & conditions of the PGCoE.
2. I/We did not submit the project proposal elsewhere for financial support.
3. I/We have explored and ensured that equipment and basic facilities will be available as and when required for the purpose of the projects.
4. I/We undertake that spare time on permanent equipment will be made available to other users.

Date: Name and Signature of Principal Investigator/s
Place:

Appendix 4

Endorsement from the Head of Institution

(To be given on institution's letter head)

Project Title:

1. Certified that the institute welcomes participation of _____as the Principal Investigator _____as the Principal Co-Investigator for the project and that in the unforeseen event of discontinuance by the Principal Investigator, the Principal Co-Investigator will assume the responsibility of the fruitful completion of the project (with due information to PGCoE).
2. Certified that the equipment and other basic facilities such other administrative facilities as per terms and conditions of the fund, will be extended to the investigator(s) throughout the duration of the project.
3. The institute assumes to undertake the financial and other management responsibilities of the project.

Date: Name and Signature of Head of Institution

Place: