PROFORMA FOR SUBMITTING R&D PROJECT PROPOSAL FOR SEEKING FINANCIAL SUPPORT

SUMMARY SHEET

1. Title of Project: **विद्युत कवच : Design and Development of a Security Operations Center (SOC) for Smart Grid**

2. Organisation

a) Name: **Sardar Patel Institute of Technology**

b) Address: Sardar Patel Institute of Technology, Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai 400058, Maharashtra, India.

c) Legal status (as per the description/provisions of Chapter 9 of General Financial Rules (GFR)-2005)

3. Chief Investigator

a) Name
b) Designation
c) Department
d) Address

4. Nature of Project (Check one)

a) Research, Development & Engineering (R,D & E) leading to production capability

b) Application oriented Research, Design and Development (R,D&D) having production potential

c) Basic R&D

5. Objective of the Project

a) Develop a reference SOC architecture for smart grid cybersecurity, aligned with CEA and CERT-In guidelines.

b) Design and validate AI/ML-based anomaly detection models for smart grid protocols (IEC-61850, DNP3, Modbus).

c) Implement User and Entity Behavior Analytics (UEBA) for insider threat and anomalous entity detection.

d) Apply aspect-based analysis on log data to derive fine-grained insights into authentication, load control, and communication anomalies.

e) Build blockchain-enabled event logging for tamper-proof forensic readiness.

f) Create automated SOAR playbooks for cyberattack scenarios.

g) Develop a hybrid testbed integrating IoT/SCADA devices with simulated smart grid environments.

h) Conduct pilot validation with utilities/industry partners.

i) Deliver training and capacity building modules.

6. Brief outline of the project with specific technology fall-outs

a) Coverage: SOC framework for smart grid cybersecurity with UEBA and aspect-based log Analysis.
b) Exclusions: Internal generation plant control systems.
c) Duration: 36 months (3 years).
d) Stakeholders: Academia, user agency, industry partners.
e) Integration: Aligned with CEA, CERT-In, NCIIPC; adaptable for SOC-as-a-Service.

7. Expected outcome in physical terms
(as applicable)
a) Specifications of subsystem/system (as applicable)
b) Nature of documents for technology transfer
c) Manpower trained

i) Level of training
ii) Nos. (industry/outside
R&D/Internal)

a) SOC prototype with SIEM-SOAR integration and UEBA modules.
b) AI/ML + UEBA models for anomaly and insider threat detection.
c) Aspect-based log analysis framework for granular forensic insights.
d) Blockchain-based secure event logging system.
e) Repository of 10+ SOAR playbooks.
f) Hybrid testbed validated with IoT/SCADA devices.
g) 5–6 IEEE/ACM publications, 1–2 patents.
h) Training of 20–25 students, 2–3 workshops with utilities.
i) Commercialization roadmap for SOC-as-a-Service.

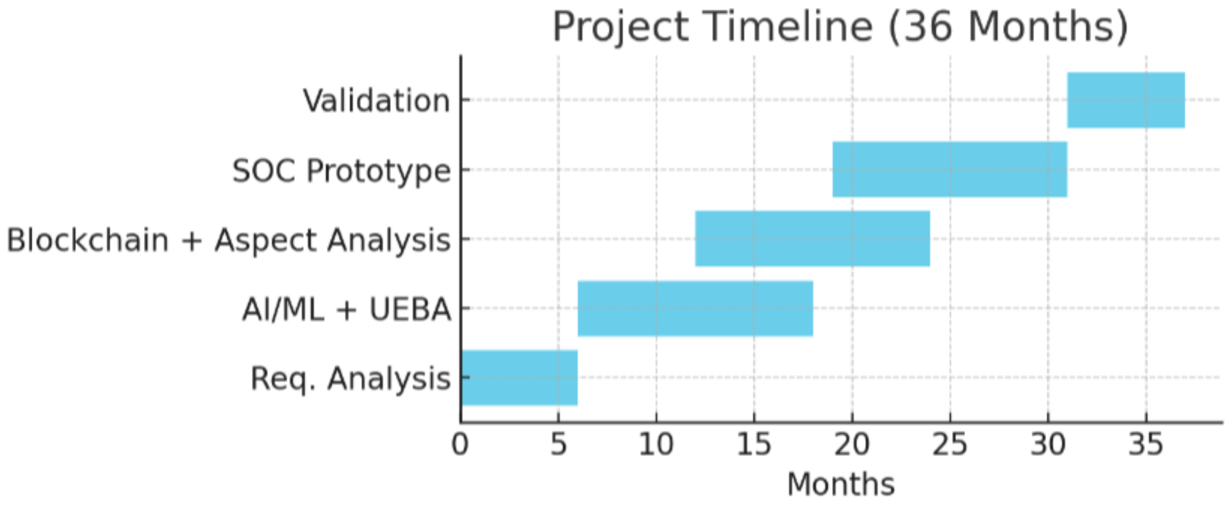
8. Agency with which link up is (Details may be given as applicable)
established/proposed

a) Utility/User Agency: Provide operational logs, testbed access, domain expertise.
b) Industry Partner: Provide UEBA/SIEM/SOAR licenses, blockchain modules, co-funding.
c) Engagement Plan: Joint validation exercises, review meetings, co-authored reports.
d) Letters of support expected from power utilities and SCADA/security vendors.

9. Duration of Project

Time Frame	**Deliverables**	**Quantifiable Outputs**
Months 1-6	Requirement analysis, SOC architecture	1 report, 1 design document

Months 7-18	AI/ML + UEBA models	3–4 models, &gt;90% accuracy, &lt;5% FPR
Months 12-24	Blockchain logging + Aspect-based analysis	1 blockchain prototype, 1 aspect-based framework
Months 19-30	SOC prototype + playbooks	1 prototype SOC, 10+ playbooks
Months 31-36	Validation, pilot testing, training	1 validation report, 2 patents, 3+ papers, 1 workshop



10. Year-wise break-up of physical achievements with specific intermediate milestones (in terms of aims and objectives)

11. Likely End User(s)

12. Name of other organisations jointly participating in the project (including organisation abroad)

13. Total Budget outlay

(Rs.in lakhs) Years

Head 1st 2nd 3rd Total Capital Equipment Rs.

Consumable stores Rs.

Manpower Rs.

Travel & Training Rs.

Contingencies Rs.

including TA/DA for
Project review meetings

Overheads, if any Rs.

<u>Grand Total</u>

` Grand Total : Rs.

14. a) Contribution of Project Implementing/ Rs.
& other Organisation in Total Budget Outlay

b) DeitY Contribution Rs.

Signature of Chief Investigator
Designation
Date

Signature of
Head of the Institution/Organisation
Designation
Date

Additional Information Required

1. Wherever applicable, Under S.No.13, share of the industry, collaborating agency, any other assistance and DeitY's support required in the total cost of the Project may be provided under various budget heads.
2. Brief history of the electronics company including products being made, capacities, related collaborators, achievements, capabilities etc. may be provided (including recent annual reports and company brochure)
3. Please indicate recent major achievements of in-house R&D Unit of the electronics company in development of new products/processes, technology export, patent taken etc. and whether in-house R&D unit of the firm is recognised by DSIR.
4. Any other information in support of the proposal.

DETAILS OF THE PROPOSAL

PART 1 : BACKGROUND INFORMATION

1. Title of Project: **विद्युत कवच : Design and Development of a Security Operations Center (SOC) for Smart Grid**

2. (i) Chief Investigator
(ii) Co-Investigator

3. Other Investigators of the Project with their designations

4. Brief Bio-data of Chief (Please attach separate sheets) Investigator and other Investigators (including
publications/patents)

5. Competence of Investigator in Project Area
(Including Industry interaction/Technology transfer)

6. Other Commitments of the Chief Investigator and
Co-Investigators (including lectures, research projects
responsibilities etc.)
Indicate the percentage of time the Chief Investigator
and Co-Investigator would devote to the project.

7. Details on each of the ongoing/completed projects
with the Chief Investigator/Co-Investigator/R&D Team

i) Project Title
ii) Funding Agency (or Internal funding)
iii) Brief Project Summary
iv) Technical Status vis-a-vis objectives
v) Financial Status (Total Project outlay, expenditure to date)
vi) Duration and year of initiation
vii) Expected date of completion

8. Brief summary of other project proposals
(submitted by any of the Investigators)
awaiting consideration of DeitY and other
funding agencies like DST, DRDO, DSIR, MHRD, ICICI, IDBI etc.

9. Infrastructure and other facilities available at the
institute for undertaking this project.

a) List of major equipment alongwith model
numbers, specifications etc.
b) Existing manpower and other personnel with
names available for the project on full-time basis.

10. Expensive Equipment /facilities available elsewhere
which could be made use of for the project.
11.Details of collaborating agencies, if any

12. Additional information, if any.

PART II : TECHNICAL INFORMATION

1. Aim and Scope of the project (in terms of specific physical achievement)

Aims:

a) Develop a reference SOC architecture for smart grid cybersecurity, aligned with CEA and CERT-In guidelines.
b) Design and validate AI/ML-based anomaly detection models for smart grid protocols (IEC-61850, DNP3, Modbus).
c) Implement User and Entity Behavior Analytics (UEBA) for insider threat and anomalous entity detection.
d) Apply aspect-based analysis on log data to derive fine-grained insights into authentication, load control, and communication anomalies.
e) Build blockchain-enabled event logging for tamper-proof forensic readiness.
f) Create automated SOAR playbooks for cyberattack scenarios.
g) Develop a hybrid testbed integrating IoT/SCADA devices with simulated smart grid environments.
h) Conduct pilot validation with utilities/industry partners.
i) Deliver training and capacity building modules.

Scope:

a) Coverage: SOC framework for smart grid cybersecurity with UEBA and aspect-based log Analysis.
b) Exclusions: Internal generation plant control systems.
c) Duration: 36 months (3 years).
d) Stakeholders: Academia, user agency, industry partners.
e) Integration: Aligned with CEA, CERT-In, NCIIPC; adaptable for SOC-as-a-Service.

2. Detailed description of the Project

Abstract:

The proposed project aims to establish a Security Operations Center (SOC) tailored specifically for India's power grids, aligning with the Central Electricity Authority (CEA) Cybersecurity Guidelines of 2021. The SOC will serve as a centralised hub for information security, equipped with an isolated and air-gapped networking system to safeguard critical infrastructure. Its primary objectives encompass proactive threat monitoring, incident response, and adherence to strict cybersecurity measures.

This initiative is pivotal in fortifying the resilience of India's power grids against evolving cyber threats. The SOC's key components include a sophisticated log-collection facility, an isolated networking system, threat monitoring and analysis, incident response protocols, and collaboration with stakeholders. The phased implementation strategy involves risk assessment, infrastructure deployment, staff recruitment, and extensive testing to ensure readiness.

The benefits are multifold, including enhanced security, continuous monitoring, and compliance with CEA guidelines. The proposal stands as an essential step towards securing the nation's critical infrastructure, ensuring a reliable and secure power supply. The project signifies a proactive investment in the stability and resilience of India's power sector, aligning with global best practices in cybersecurity for critical infrastructure.

Idea Description:

The project aims to establish a cutting-edge Security Operations Center (SOC) dedicated to fortifying the cybersecurity infrastructure of India's power sector, adhering to the Central Electricity Authority (CEA) Cybersecurity Guidelines of 2021. The SOC will house a centralised information security log-collection facility, leveraging an isolated and air-gapped networking system. By implementing robust security measures, this initiative will fortify the nation's power grids against cyber threats, ensuring uninterrupted and secure energy supply to citizens.

Introduction:

Cybersecurity threats pose a significant risk to critical infrastructure, particularly the power sector. The Central Electricity Authority's 2021 guidelines underscore the urgency of fortifying the cybersecurity framework within this sector. To address these challenges, we propose the establishment of a Security Operations Center (SOC) tailored specifically for India's power grids.

Problem Statement:

Current smart grid infrastructures in India face challenges such as:

1) Limited visibility into network traffic across distributed energy resources.
2) Absence of centralized monitoring for cyber-physical threats.
3) Inadequate mechanisms for early detection of anomalies (e.g., false data injection, load manipulation).
4) Lack of integration between operational technology (OT) and information technology (IT) security systems.
5) Regulatory pressure from agencies like CERC, CEA, and BIS, as well as alignment with MeitY’s cybersecurity initiatives.

There is a pressing need to design a dedicated SOC framework that addresses the unique requirements of smart grid environments.

3. Need, forecast and urgency for the technology proposed to be developed with justification such as importance of know-how, import substitution role, pay off w.r.t. purchase of know-how or development of technology competitiveness, technology exports, international alliances possibilities etc.

4. Specific manner in which knowhow generated here is
envisaged to be translated into production, details regarding

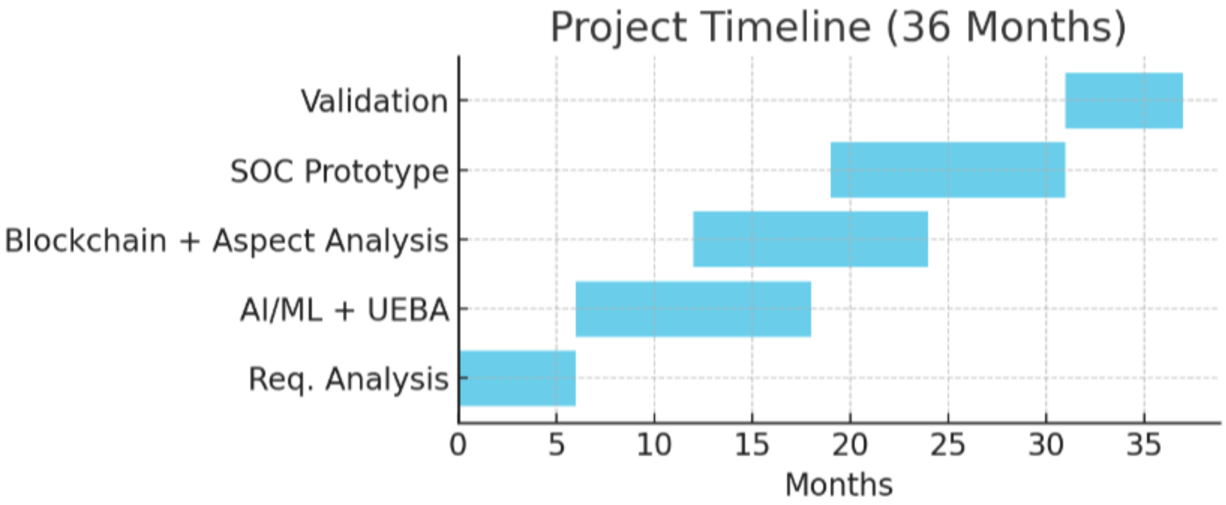
a) the end product (with specifications to be attained etc.)
b) availability of pilot production facility in the organisation

5. a) Name of production agencies willing to productionise/use and market surveys if any made by them regarding demand for the product

b) Alternative production/user agencies.

6. Period required for completing the project

Time Frame	Deliverables	Quantifiable Outputs
Months 1-6	Requirement analysis, SOC architecture	1 report, 1 design document
Months 7-18	AI/ML + UEBA models	3–4 models, &gt;90% accuracy, &lt;5% FPR
Months 12-24	Blockchain logging + Aspect-based analysis	1 blockchain prototype, 1 aspect-based framework
Months 19-30	SOC prototype + playbooks	1 prototype SOC, 10+ playbooks
Months 31-36	Validation, pilot testing, training	1 validation report, 2 patents, 3+ papers, 1 workshop



7. Details of work already done by present investigators/R&D team in this or other areas

a) Successfully completed on schedule
b) Currently in progress
c) Abandoned
d) Industry interaction/knowhow transferred

8. Summary of similar work being done elsewhere in the country

9. Information regarding specific intermediate milestones (year-wise)

10. a) Specific problems, hold-ups and difficulties foreseen in the implementation of the project.

b) If the answer is not Nil to 10(a), how does Chief Investigator propose to overcome them?

11. Detailed PERT/BAR Chart (Separate Sheet)

12. Details of possible alternative arrangements if the Chief Investigator leaves institution or is unable for any other reason to continue on this project.

13. Name of other organisations in India or Abroad jointly participating in this effort, extent of their involvement, specific division of responsibility, accountability etc.

14. List the personnel already working in the organisation who would be transferred to work full time on this project.

15. Name of experts whom the Chief Investigator would invite to join the project team as full time/part time member.

PART III - FINANCIAL DETAILS

Table - 1 Yearly Break-up

Year	Cost to MeitY	Cost to Institution (SPIT)	Total
Year 1	72	18	90
Year 2	53	13	66
Year 3	33	11	44
Total	**160**	**42**	**200**

Subsystem	MeitY Support	Institutional Contribution	Total
A. Hardware & Testbed Setup (GPU servers, IDS/IPS, SCADA kits, Smart Meters, PMUs, Networking)	55	12	67
B. Software & Tools (SIEM/SOAR, UEBA modules, Blockchain platform, Simulators, Cloud credits)	15	5	20
C. Manpower (1 RA, 2 JRFs, interns, support staff)	42	10	52

D. Travel & Collaboration (utility visits, industry meetings, conferences)	12	2	14
E. Training & Workshops (Bootcamps, professional courses, student workshops)	5	2	7
F. Publications & IPR (open-access, patent filing)	8	2	10
G. Contingency	6	1	7
H. Institutional Overheads	17	8	25
Total	**160**	**42**	**200**

Designation	No. of Posts	Monthly Emoluments (₹)	Duration	Total Cost (₹ Lakhs)
Research Associate (RA)	1	60,000	36 months	21.6
Junior Research Fellow (JRF)	2	37,000	36 months	26.6
Interns / Project Assistants	2	10,000	24 months	4.8
Support/Technical Staff	1	25,000	24 months	7.2
Total	**6**	—	—	**60.2**

Budget requirements for the Year 1 (Please provide separate breakup for each year of the project duration)

S.No.	Head	Local expenses	Foreign Exchange (FE)	Duty	Total	Part of 6 to be borne by participating/	Amount payable
						by MeitY other expenses	
1.	2.	3.	4.	5.	6.	7.	8.
1.	Capital Equipment	40	4	1	5	DeitY-35, SPIT-10	45
2.	Consumable 5	5	0	0	5	DeitY-4, SPIT-1	5

	stores						
3.	Manpower	30	0	0	30	DeitY-24, SPIT-6	30
4.	Travel/ Training	5	0	0	5	DeitY-4, SPIT-1	5
5.	Contingencies other expenditure debitable to this project	3	0	0	3	DeitY-3, SPIT-0	3
6.	Overhead, if any	2	0	0	2	DeitY-2, SPIT-0	2

Total: Rs. 90 Others: Rs.18 DeitY. Rs. 72

Budget requirements for the Year 2 (Please provide separate breakup for each year of the project duration)

S.No.	Head	Local expenses	Foreign Exchange (FE)	Duty	Total	Part of 6 to be borne by participating/	Amount payable
						by MeitY other expenses	
2.	2.	3.	4.	5.	6.	7.	8.
7.	Capital Equipment	20	2	1	3	DeitY-20, SPIT-5	25
8.	Consumable stores	3	0	0	3	DeitY-2, SPIT-1	3
9.	Manpower	30	0	0	30	DeitY-24, SPIT-6	30
10.	Travel/ Training	3	0	0	3	DeitY-2, SPIT-1	3
11.	Contingencies other expenditure debitable to this project	3	0	0	3	DeitY-3, SPIT-0	3
12.	Overhead, if any	2	0	0	2	DeitY-2, SPIT-0	2

Total: Rs.66 Others: Rs. 13 DeitY. Rs. 53

Budget requirements for the Year 3 (Please provide separate breakup for each year of the project duration)

S.No.	Head	Local expenses	Foreign Exchange	Duty	Total	Part of 6 to be borne	Amount payable

			(FE)			by participating/	
						by MeitY other expenses	
3.	2.	3.	4.	5.	6.	7.	8.
13.	Capital Equipment	12	2	1	3	DeitY-9, SPIT-6	15
14.	Consumable stores	5	0	0	5	DeitY-4, SPIT-1	5
15.	Manpower	15	0	0	15	DeitY-12, SPIT-3	15
16.	Travel/ Training	3	0	0	3	DeitY-2, SPIT-1	3
17.	Contingencies other expenditure debitable to this project	3	0	0	3	DeitY-3, SPIT-0	3
18.	Overhead, if any	3	0	0	3	DeitY-3, SPIT-0	3

Total: Rs. 44   Others: Rs. 9 DeitY. Rs. 35

- All figure in INR lacs

Table II : Subsystem wise Break-up

S.No. Item description (including test Total cost equipment, components, materials etc.)

1 2 3 1.

2.

3.

Grand Total :

S.No.	**Item description (including test equipment, components, materials etc.)**	**MeitY (₹ Lacs)**	**SPIT (₹ Lacs)**	**Total (₹ Lacs)**
1	**Hardware & Testbed Setup – GPU Servers (AI/ML), IDS/IPS Appliances, SCADA Training Kits, Smart Meters, PMUs, Networking Switches & Firewalls**	**44.66**	**11.17**	**55.83**
2	**Software & Tools – SIEM/SOAR Platform Licenses, UEBA Modules, Blockchain Test Platform, Protocol Simulators (IEC-61850, DNP3, Modbus), Cloud Compute Credits**	**13.34**	**3.33**	**16.67**
3	**Travel & Collaboration – Utility site visits, Industry partner meetings, National conferences**	**9.34**	**2.33**	**11.67**
4	**Training & Workshops – Bootcamps, Professional certification courses, Student workshops**	**4.66**	**1.17**	**5.83**

5	**Publications & IPR – Open-access journal fees, IEEE/ACM conference registration, Patent filing charges**	**6.66**	**1.67**	**8.33**
6	**Contingency – Miscellaneous project support costs**	**4.66**	**1.17**	**5.83**
7	**Institutional Overheads – Institute charges (electricity, administration, audit, etc.)**	**16.67**	**4.17**	**20.84**
	Subtotal (Non-Manpower)	**100.00**	**25.00**	**125.00**

Grand Total : 125 lacs

Table-III Manpower Details

S.No. Designation/ Monthly Ist Year 2nd Year Total Salary salary
Scientific/ No.of Total No.of Total Technical Posts Posts Expenditure posts Expenditure 1
2 3 4 5 6 7 8

AI/ML Researcher - Rs 60k/m
Blockchain Developer Rs 60k/m
Embedded Systems Engineer Rs 60k/m
Project Manager Rs 70k/m

S.No.	Designation	No. of posts	Monthly Salary (₹)	Duration	Total Cost (₹ Lacs)	Description

1	Research Associate (RA)	1	60,000	36 months	26.91	PhD/postdoc-level researcher to coordinate the project, lead AI/ML & blockchain development, manage collaborations, and prepare publications & patents.
2	Junior Research Fellows (JRF)	2	37,000	36 months	33.14	Two postgraduate researchers to design SOC modules, develop UEBA & anomaly detection models, run experiments on SCADA/IoT testbeds, and contribute to training workshops.
3	Interns / Project Assistants	2	10,000	24 months	5.98	Undergraduate interns/assistants to support coding, data collection, simulation experiments, report preparation, and assist in workshop delivery.

4	Support / Technical Staff	1	25,000	24 months	8.97	Technical staff for system administration, testbed maintenance (GPU servers, SCADA kits, PMUs), procurement, and lab management.
	Total (Manpower)				75.00	

- Manpower funding split: MeitY = 60.58 Lacs, SPIT = 14.42 Lacs
- Year-wise manpower allocation: Year1 = 30.00 Lacs, Year2 = 30.00 Lacs, Year3 = 15.00 Lacs
- Total: 75 lacs