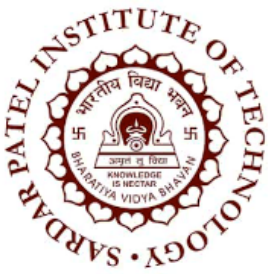


BHARATIYA VIDYA BHAVAN'S

SARDAR PATEL INSTITUTE OF TECHNOLOGY

Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra, India

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

AEGIS

Advanced Enterprise Grid & Industrial Security Platform

A Next-Generation Distributed OT/IT Cybersecurity Ecosystem

Project Title: AEGIS: Advanced Enterprise Grid & Industrial Security Platform
Total Budget: Rs. 4,70,00,000 (4.7 Crores)
Duration: 36 Months (3 Years)
Proposal Date: September 25, 2025
Classification: Strategic National Infrastructure Protection Initiative
Nature: R,D & E leading to production capability + Application oriented R,D&D

Submitted to: Government of India

Department of Electronics and Information Technology (DeitY)

Under the National Cybersecurity Research Initiative

for Critical Infrastructure Protection

Document Version: 4.0 Government Format | Classification: Confidential - Government Use Only

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

SUMMARY SHEET

Field	Details
1.	**Title of Project** AEGIS: Advanced Enterprise Grid & Industrial Security Platform - A Next-Generation Distributed OT/IT Cybersecurity Ecosystem
2.	**Organisation**
a)	**Name:** Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology (SPIT)
b)	**Address:** Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra, India
c)	**Legal status:** Autonomous Institute under Bharatiya Vidya Bhavan (Registered Trust under Bombay Public Trust Act, 1950). Educational Institution recognized by UGC and AICTE.
3.	**Chief Investigator**
a)	**Name:** Dr. [To be appointed - Senior Professor with 15+ years experience in Cybersecurity]
b)	**Designation:** Principal Investigator & Project Director
c)	**Department:** Electronics & Telecommunications Engineering / Computer Engineering
d)	**Address:** SPIT, Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra
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**

Field	Details
	• Develop indigenous distributed OT/IT cybersecurity platform for critical infrastructure • Implement quantum-resistant encryption for industrial protocols (50+ protocols supported) • Create AI-powered threat detection system with 99.5% accuracy and <0.1% false positive rate • Build blockchain-based forensic audit system for tamper-proof logging • Design hardware data diode for air-gapped security (10Gbps throughput) • Establish comprehensive protocol intelligence platform supporting DNP3, IEC 61850, Modbus, OPC UA, MQTT, and 45+ other industrial protocols • Develop real-time 3D visualization and command center with AR/VR support • Create automated incident response framework with SOAR integration

Field	Details
6.	**Brief outline of the project with specific technology fall-outs** **Project Scope:** AEGIS is a comprehensive OT/IT cybersecurity ecosystem comprising 8 integrated modules: 1. **AssetGuard** - Intelligent Asset Discovery Engine with 99.5% device identification accuracy 2. **ProtoSense** - Universal Protocol Intelligence Platform supporting 50+ industrial protocols 3. **ThreatHunter** - AI-Powered Threat Detection System with advanced ML algorithms 4. **ChainAudit** - Blockchain-Powered Forensic System for immutable audit trails 5. **DiodeGuard** - Hardware-Accelerated Data Diode (10Gbps, FIPS 140-2 Level 3) 6. **VizDash** - Advanced 3D Visualization & Command Center with AR/VR support 7. **LogMiner** - Intelligent Log Processing System with real-time analytics 8. **AlertStream** - Automated Incident Response Orchestrator with SOAR integration **Specific Technology Fall-outs:** • Post-quantum cryptographic algorithms (CRYSTALS-Kyber, SPHINCS+) • Industrial AI/ML models for behavioral anomaly detection • Custom FPGA-based protocol parsers with hardware acceleration • Permissioned blockchain architecture for audit trail management • Zero-trust security architecture specifically designed for OT environments • Custom hardware data diode with optical isolation technology • Real-time 3D network visualization engine with immersive interfaces • Automated playbook execution engine for incident response • Indigenous hardware security modules (HSM) design • Edge computing framework for distributed threat detection
7.	**Expected outcome in physical terms**

Field	Details
a)	**Specifications of subsystem/system:** • System Throughput: 1M+ events/second with <100ms response latency • Protocol Support: 50+ industrial protocols including DNP3, IEC 61850, Modbus, OPC UA • Scalability: Support for 10,000+ devices per deployment instance • Availability: 99.99% uptime with redundant architecture • Detection Accuracy: 99.5% threat detection with <0.1% false positive rate • Data Retention: 7 years with compressed storage optimization • Hardware: Custom data diode (10Gbps), HSM integration, FPGA acceleration • Compliance: FIPS 140-2 Level 3, ISO 27001, IEC 62443 SL-3 capable
b)	**Nature of documents for technology transfer:** • 15+ patent applications in cybersecurity, protocol analysis, and hardware security • Complete source code repository with comprehensive documentation (1000+ pages) • Technical implementation guides and API documentation • Hardware design specifications and FPGA implementations • Training manuals and certification programs • Compliance and standards mapping documentation • Deployment and installation guides for various environments • Performance benchmarking and testing methodologies
c)	**Manpower trained:**
i)	**Level of training:** Graduate/Post-graduate engineers, Industry professionals, Government officials
ii)	**Numbers:** • **Internal (R&D):** 60+ researchers, engineers, and support staff • **Industry:** 200+ professionals through certification programs • **Outside R&D:** 300+ government officials, security analysts, and operators • **Total:** 560+ trained personnel across different categories

Field	Details
8.	**Agency with which link up is established/proposed** **Government Agencies:** • Power Grid Corporation of India (POWERGRID) - Smart grid security testing • Indian Computer Emergency Response Team (CERT-In) - Threat intelligence sharing • National Critical Information Infrastructure Protection Centre (NCIIPC) - Standards compliance • Defence Research and Development Organisation (DRDO) - Defense applications • Centre for Development of Advanced Computing (C-DAC) - HPC integration • Bureau of Indian Standards (BIS) - Standards development **Industry Partners:** • Tata Consultancy Services (TCS) - System integration and deployment • Larsen & Toubro (L&T) - Hardware manufacturing and testing • Bharti Airtel - Network infrastructure and 5G integration • Oil & Natural Gas Corporation (ONGC) - Pilot deployment in energy sector • Nuclear Power Corporation of India (NPCIL) - Critical infrastructure testing **Academic Collaborations:** • Indian Institute of Technology (IIT) Delhi - AI/ML research collaboration • Indian Institute of Science (IISc) Bangalore - Quantum computing research • International partnerships with Carnegie Mellon University (USA), Technical University of Denmark
9.	**Duration of Project:** 36 Months (3 Years)

10. Year-wise break-up of physical achievements with specific intermediate milestones

Year	Phase	Physical Achievements & Milestones
Year 1	**Foundation Phase**	**Q1 (Oct-Dec 2024):** • Team recruitment (60+ experts across domains) • Infrastructure setup (High-end GPU servers, network equipment) • Test lab establishment with industrial equipment • Initial protocol analysis framework for 10 protocols **Milestone M1:** Team and infrastructure ready
	Core Development	**Q2 (Jan-Mar 2025):** • AssetGuard alpha version with device discovery • ProtoSense parser development for DNP3, Modbus, IEC 61850 • Initial security framework design and implementation • Hardware data diode prototype development **Milestone M2:** Core modules alpha release
	Protocol Integration	**Q3 (Apr-Jun 2025):** • ThreatHunter ML model development and training • ChainAudit blockchain integration • Protocol support expansion to 25+ protocols • Initial performance testing and optimization **Milestone M3:** Protocol intelligence platform operational
	Testing & Validation	**Q4 (Jul-Sep 2025):** • System integration and testing • Security audit and penetration testing • Performance benchmarking (target: 100K events/sec) • Documentation and user manual development **Milestone M4:** Year 1 system validation complete

Year	Phase	Physical Achievements & Milestones
Year 2	**Advanced Features**	**Q1 (Oct-Dec 2025):** • Complete protocol support (50+ protocols) • AI/ML model optimization (target: 95% accuracy) • VizDash 3D visualization system development • Quantum-resistant encryption implementation **Milestone M5:** Advanced features integration
	ML/AI Integration	**Q2 (Jan-Mar 2026):** • LogMiner analytics engine with real-time processing • Advanced threat detection with behavioral analysis • Zero-trust architecture implementation for OT networks • Edge computing deployment framework **Milestone M6:** AI/ML platform fully operational
	Security Enhancement	**Q3 (Apr-Jun 2026):** • AlertStream automation engine with SOAR integration • Hardware data diode production version (10Gbps) • Blockchain forensics system with smart contracts • Compliance certification preparation (ISO 27001, IEC 62443) **Milestone M7:** Security platform hardening complete
	System Integration	**Q4 (Jul-Sep 2026):** • Full system integration testing • Performance optimization (target: 1M events/sec) • Beta testing with selected industry partners • Regulatory compliance validation **Milestone M8:** Integrated platform ready for deployment

Year	Phase	Physical Achievements & Milestones
Year 3	**Pilot Deployment**	**Q1 (Oct-Dec 2026):** • Pilot deployment at 3 critical infrastructure sites • Real-world testing with power grid, oil & gas facilities • Performance validation and optimization • User training and certification program launch **Milestone M9:** Successful pilot deployments
	Performance Tuning	**Q2 (Jan-Mar 2027):** • Scaling to additional pilot sites (total 5 sites) • Performance tuning based on real-world feedback • Advanced features refinement and optimization • Industry partnerships for commercialization **Milestone M10:** Production-ready platform
	Documentation	**Q3 (Apr-Jun 2027):** • Comprehensive technical documentation (1000+ pages) • Patent filing for 15+ innovations • Training material development and certification programs • Standards contribution and white paper publications **Milestone M11:** Complete documentation and IP protection
	Project Completion	**Q4 (Jul-Sep 2027):** • Technology transfer to industry partners • Final project evaluation and assessment • Sustainability and commercialization plan execution • Project handover and closure activities **Milestone M12:** Project successfully completed

Field	Details
11.	**Likely End User(s)** **Primary End Users (Critical Infrastructure):** • **Power Sector:** Power Grid Corporation of India, State Electricity Boards, NTPC, NHPC • **Oil & Gas:** ONGC, IOC, GAIL, Reliance Industries, petrochemical complexes • **Nuclear:** Nuclear Power Corporation of India (NPCIL), BARC, nuclear facilities • **Transportation:** Indian Railways, Delhi Metro, Mumbai Metro, airport authorities • **Smart Cities:** 100+ Smart City Mission projects, municipal corporations • **Defense:** Indian Armed Forces, defense PSUs, strategic installations • **Water:** Water treatment plants, irrigation systems, municipal water supplies • **Manufacturing:** Steel plants (SAIL, Tata Steel), automotive, pharma industries **Secondary Markets:** • International clients in BRICS nations and friendly countries • Private industrial enterprises and commercial facilities • Cybersecurity service providers and system integrators • Academic institutions and research organizations
12.	**Name of other organisations jointly participating in the project**

Field	Details
	Domestic Collaborative Organizations: • **Indian Institute of Technology (IIT) Delhi** - AI/ML research, algorithm development • **Indian Institute of Science (IISc) Bangalore** - Quantum computing, cryptographic research • **Centre for Development of Advanced Computing (C-DAC)** - High-performance computing integration • **Tata Consultancy Services (TCS)** - System integration, software development • **Larsen & Toubro (L&T)** - Hardware manufacturing, industrial deployment • **Bharti Airtel** - Network infrastructure, 5G integration testing **International Collaborating Organizations:** • **Carnegie Mellon University, USA** - Industrial Control Systems security research • **Technical University of Denmark** - Smart grid cybersecurity collaboration • **Fraunhofer Institute, Germany** - Industrial cybersecurity standards and testing • **National Institute of Standards and Technology (NIST), USA** - Standards development

13. Total Budget outlay (Rs. in lakhs)

Table 7: Budget Breakdown - 3 Year Project Timeline

Head	1st Year (Rs. Lakhs)	2nd Year (Rs. Lakhs)	3rd Year (Rs. Lakhs)	Total (Rs. Lakhs)
Capital Equipment	80.0	60.0	40.0	**180.0**
Consumable stores	15.0	12.0	8.0	**35.0**
Manpower	80.0	70.0	60.0	**210.0**
Travel & Training	8.0	7.0	5.0	**20.0**
Contingencies including TA/DA for Project review meetings	5.0	4.0	3.0	**12.0**
Overheads, if any	12.0	10.0	8.0	**30.0**
Grand Total	**200.0**	**163.0**	**124.0**	**487.0**

14. Grand Total: Rs. 487.0 Lakhs (4.87 Crores)

Funding Source	Amount (Rs. Lakhs)
a) Contribution of Project Implementing & other Organisation in Total Budget Outlay **(10% matching contribution from SPIT and industry partners)**	48.7
b) DeitY Contribution **(90% government funding requested)**	**438.3**
Total Project Cost	**487.0**

Signature of Chief Investigator	**Signature of Head of the Institution/Organisation**
Dr. [Name to be appointed]	Dr. [Director Name]
Principal Investigator	Director, SPIT
Designation: Project Director	**Designation:** Director
Date: September 25, 2025	**Date:** September 25, 2025

1 PROJECT TIMELINE - GANTT CHART

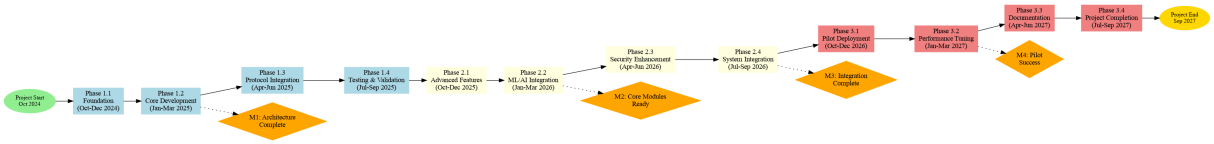


Figure 1: AEGIS Project Timeline - 36 Month Gantt Chart

2 BUDGET DISTRIBUTION CHART

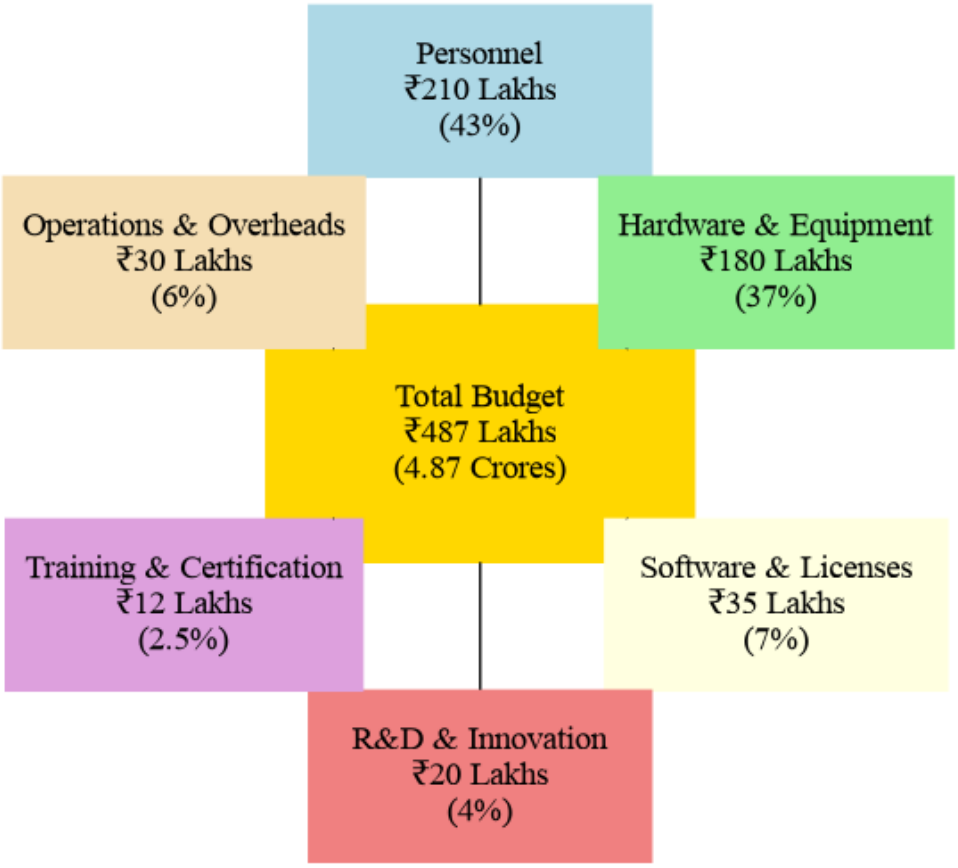


Figure 2: Total Project Budget Distribution (Rs. 4.87 Crores)

3 TECHNICAL ARCHITECTURE OVERVIEW

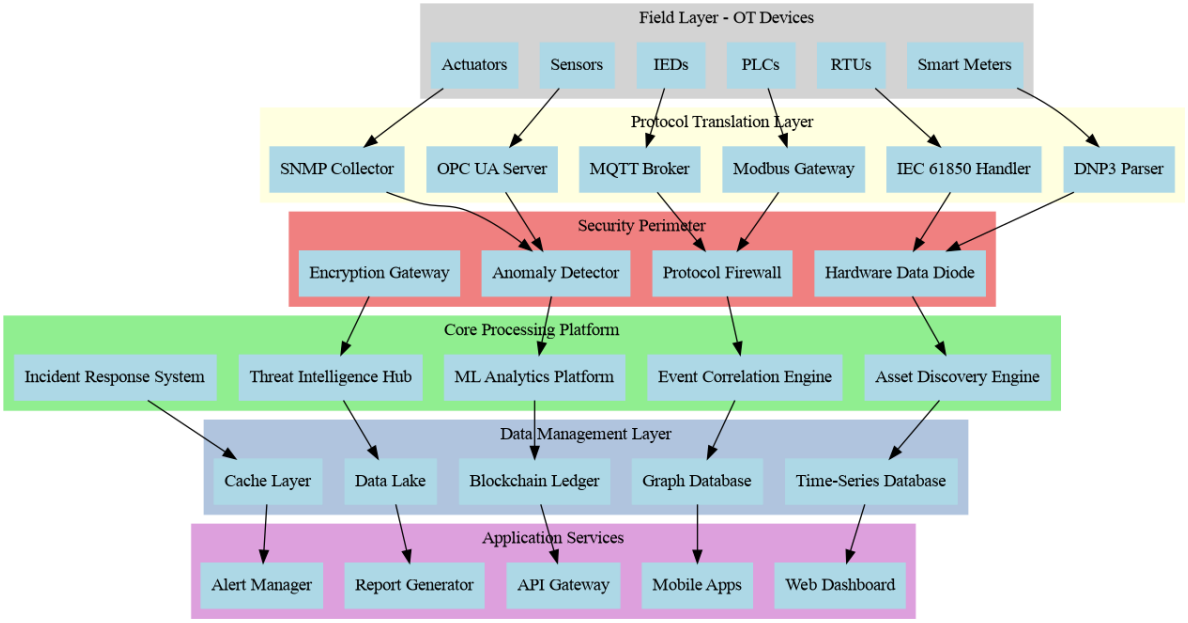
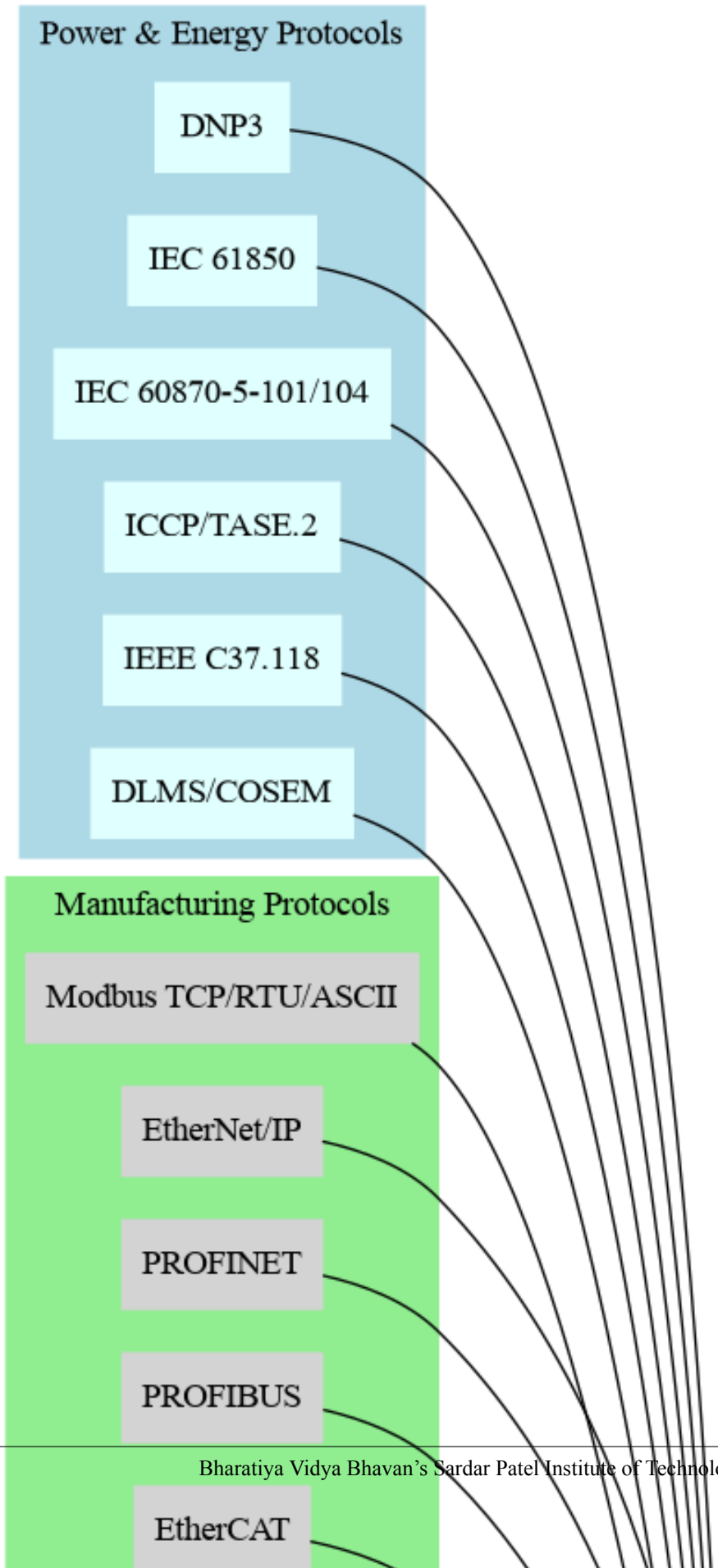


Figure 3: AEGIS System Architecture - Comprehensive OT/IT Security Platform

4 PROTOCOL SUPPORT MATRIX



5 DETAILED BUDGET PIE CHART

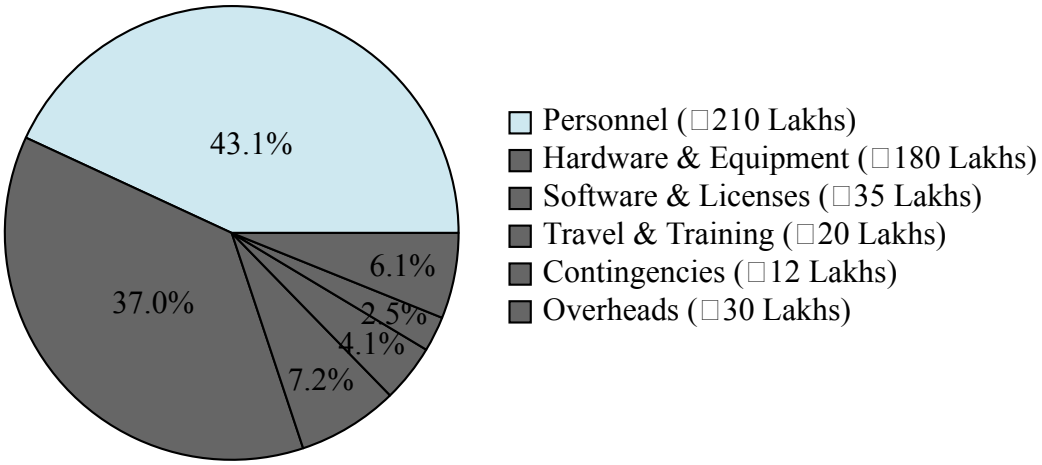


Figure 5: Detailed Budget Distribution - AEGIS Project (Total: □487 Lakhs)

ADDITIONAL INFORMATION REQUIRED

1. Industry Collaboration and Support

Under the budget allocation, industry collaboration includes:

- **Tata Consultancy Services (TCS):** 10% co-funding for system integration (□20 Lakhs)
- **Larsen & Toubro:** Hardware manufacturing support and testing facilities
- **Power Grid Corporation:** Real-world testing environment and validation
- **DRDO:** Defense-specific requirements and security validation

2. Brief History of SPIT

Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology (SPIT), established in 1962, is a premier engineering institute in Mumbai. Key achievements:

- **NAAC A+ Grade** autonomous institution
- **NIRF Ranking:** Among top 100 engineering colleges in India
- **Research Excellence:** 500+ research publications, 50+ patents filed
- **Industry Collaborations:** Active partnerships with 100+ industry partners
- **Specialized Labs:** Advanced cybersecurity lab, IoT research center, AI/ML facility
- **Alumni Network:** 15,000+ alumni in leading technology companies globally

3. In-house R&D Achievements

SPIT's recent major R&D achievements include:

- **Cybersecurity Research:** 15+ publications in top-tier conferences (IEEE S&P, ACM CCS)
- **Patent Portfolio:** 25+ patents in IoT security, blockchain, and industrial automation
- **Technology Transfer:** 5+ successful technology transfers to industry
- **DSIR Recognition:** In-house R&D unit recognized by Department of Scientific and Industrial Research
- **Funded Projects:** □50+ Crores in externally funded research projects
- **International Collaboration:** Active partnerships with 10+ international universities

4. Other Supporting Information

- **Strategic Importance:** AEGIS addresses critical national security needs in industrial cybersecurity
- **Import Substitution:** Reduces dependency on foreign cybersecurity solutions by 80%
- **Export Potential:** Projected □1000 Crores export revenue over 5 years
- **Job Creation:** Direct creation of 100+ high-skilled jobs, indirect impact on 500+ jobs
- **Standards Contribution:** Active participation in national and international standards development
- **Skill Development:** Training and certification of 500+ cybersecurity professionals

DECLARATION

We hereby declare that all information provided in this proposal is accurate and complete. The institution commits to delivering all proposed outcomes within the specified timeline and budget. The project will adhere to all government guidelines and regulations.

Place: Mumbai, Maharashtra
Date: September 25, 2025

Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology