EasyChair Preprint

№ 2164

Risk Management in Automation for Power Trading

Pradip Banerjee, Anindita Banerjee and Anindita Ganguly

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

December 13, 2019

Risk Management in automation for power trading

Pradip Banerjee, Anindita Banerjee, Anindita Ganguly

***Abstract*— Abstracts: Electric Power is a global business. Over the years, many countries, including India, have ceded ownership of power and automation firms to the private sector. Such an environment opens up opportunities for increased profit generation. Modern power and automation technologies ensure not only focus on production efficiency but also ensure that an intricate balance is achieved between production and consumption. These technologies, however, are not without challenges and hence risks**

While automation is known to enhance safety and system reliability, such systems are more vulnerable to intrusion and thus, elimination of one risk yields a newer form of risk. For instance, buying, selling, and distributing power require an interconnected transmission line based on computer management operations. Such operations are prone to cyber intrusion and hence, the increased need for advanced risk management procedures.

Keywords—: Electricity, Automation, HMI, ABT, IPP

Prologue: Electric energy value chain begins with the source of energy: Fuel source –Transportation of fuel to Power Plant –Production of commodity, Electricity –Transmission –Consumption by Byers. Unlike other commodities, Electricity cannot be stored [5]. Thus, every moment total power generated in a particular grid must be equal to the total demand (consumption). The lack of electricity transmission / distribution infrastructure has made business of the independent power plant (IPP) and the byers (consumers) nervous about whether their need will be met. Consequently, all the IPPs in that particular grid would try to sell maximum power, which each is capable to generate. Further the consumers having power purchase agreement (PPA) with some IPP or Distribution Company may consume more / less power than that each agrees. These would cause Grid discipline (Frequency may increase / decrease from the nominal value). To avoid such eventuality every country makes Grid Regulations and Availability based Tariff (ABT) for both the Generating Companies and Consumers[11]..

Under the above scenario, Automation pitched in the Power Generating Units for Power trading. The advanced technologies generally involve human-machine interaction (HMI) systems that ensure not only focus on production efficiency but also ensure that an intricate balance is achieved between production and consumption, which however, are not without challenges and hence risks [1]. Such operations are prone to cyber intrusion and hence, the increased need for advanced risk management procedure.

Risk management in Power Industry: The risk management process has undergone rapid evolution since the last century. Its evolution has seen its transformation from a perfunctorily employed activity to a critical requirement in enterprise management. Recognition and mitigation of risks, regulations compliance, increased market valuation, and asset usage optimization have been incorporated into the risk management process [4]. Unlike risk managers in other industrial sectors who have to deal only with real-time risk measurement and mitigation, risk managers in power and automation industries have to deal with increased complexities due to its inherent nature. Optimization of returns and minimization of risks in plant usage, delivery schedules, market balance and cash flows remains a formidable task that the managers have to reckon with [2].

Power and automation industries just like any other industries are keen to ensure that risks involved are kept at minimal. The global industrial environments require managers take into consideration all the risk dimensions including safety-related risks. To stay competitive, industries must integrate production, safety-related and economic risks management as a tool to efficiency [12].. Integrated risk management in powered and automation industries brings about increased benefits including clearer decision making criteria, effective investment usage, cost consciousness and increased innovation in achievement of production goals, improved communication among all production levels and organization stakeholders, and enhanced focus on safety in relation to environment, legislations, and economic situations

Many countries are currently exercising increased roles in enhancing automation within power industries. Moreover, respective regional bodies have developed stringent compliance and regulatory guidelines Additionally, state and public service commissions continuously make policy changes that increase challenges for power and automation industries risk managers. infrastructure protection (CIP) reliability standards which obliges industrial players to meet [3] However, such rigid compliance requirement has proven onerous to the industrial players, hence giving rise to legal risks by the players.

Surviving in the resulting deregulated environments requires the power and automation industries to not only preserve safety but also focus on market variations and firm performance While such an environment is accompanied by risks, it opens up opportunities for increased profit generation. It is on the context that the industry players need to take into consideration all risk aspects and in turn, develop practicable solutions which do not compromise safety and industrial performance efficiency [6]

The research e analysis approach enables determination of appropriate mixture of prevention measures and risk transfer and retention by the organization. This is expected to established that power industries with increased safety measures recorded low operation and maintenance costs per kilowatt-hour. In another research, it was established that an integrated risk analysis

approach enables determination of appropriate mixture of prevention measures and risk transfer and retention by the organization. This is expected to result in accrued stakeholder benefit. Effective risk management involves the following strategies [7].

1. Understanding the risk
2. Organizations' self-awareness and hence building of protection strategies
3. Increased awareness and quick responses
4. Security posture sustenance
5. Understanding the risk
6. Organizations' self-awareness and hence building of protection strategies
7. Increased awareness and quick responses

Based on these risks, firms have shifted focus to systematic identification, measurement, prioritization, and response to all the risks they face. A deeper investigation of risk management process reveals a cycle of process that gives rise to the whole process (see illustration below)

.

Figure1=Risk Management Cycle

The Risk: The global power and automation industry is subject to price, supply, and consumption matters. The power and automation companies are additionally faced by political, regulatory, and legal risks along every aspect of their operations. International operated companies face an increased load of risks through its susceptibility to commercial and security threats resulting from inconvertibility/transfer restrictions of currencies, contract breaches, confiscation/nationalization threats (creeping expropriation of assets), and wars/civil unrests These issues bedevil risk managers and are subject to critical decision-making processes. Additionally, the managers face difficulty in determining the real threats to a company between the constantly changing scenarios and immense real-time data availability. Discrimination between the varying threats and hence their relative importance remains a great challenge to the risk managers in power plants. Prioritization is also of fundamental question to such managers. Risk management attempts to answer these questions through a guided framework Management of risks involves discovery of individual industry assets and understanding the weaknesses, expected losses, and appropriate tactics in mitigating the risks to ensure sustained values. The IEEE standard 15408 defines a common criteria risk assessment table that assists in depicting relationship of owners value to firm assets with respect to possible risks. (see figure below)

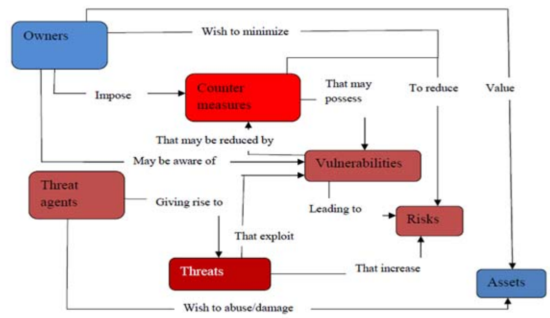

Figure 2: Threat reduction flow chart

The diagram described above illustrates a process aimed at threat-agent restriction, hence reduced exploitation of threats that pose vulnerabilities to the industries assets

Discovering Industry Assets, their Weaknesses and Capabilities: Assets in power and automation industries are typically adequately engineered and documented at initiation. However, such industries undergo replacement, upgrade, personnel changes and hence, initially documented information may be inaccurate and inappropriate. The need for constant documentation and identification of emerging weaknesses and capabilities to functionality is therefore paramount. Moreover, asset identification process involves documentation review, physical inspection, industry analysis, and interview of personnel. This facilitates a wholesome discovery of industry assets comprising their architecture within the industry. Such a process needs to take into account weakness areas, which threaten the critical functionality of the physical assets within the industry. Such assets include power generation appliances, automation hardware and software, security systems, and other supportive physical assets.

Risk definition and identification: Generally, risks are based on change potential and the consequent magnitude of such changes. Each industrial discipline independently defines risk in a manner that reflects its focus parameters and consequences. However, all definition converges toward encompassment of the frequency and consequence elements that constitute the risk. For a power and automation risk analyst, risk is defined within the context of ending up with a system that maximally utilizes power generation resources within the precinct of the stipulated regulatory standards in the relevant region. A nuclear safety analyst will on the other hand define risk within the context of developing a system that generates a frequency of radioactive releases that fall within the minimum requirements of both institutional and regulatory objectives. However, a financial analyst will look at the possibility that some factors will bar investment costs from being recovered over a specified period of time. All these definitions encompass the key aspects of risk management and hence, the four classifications are safety-related risks, operations risks, financial risks, and strategic risks.

Framework for Risk Management in Power and Automation Industries: As mentioned earlier, risk management in power and automation industries is viewed as constituting safety, operational and financial risks embedded within the organizations strategic environment. As seen in Figure 3 below, the risk areas intersect each other with a decision in one area affecting the risk vulnerability in another area. In addition, the framework outlines the key stakeholders who affect the three risk areas identified

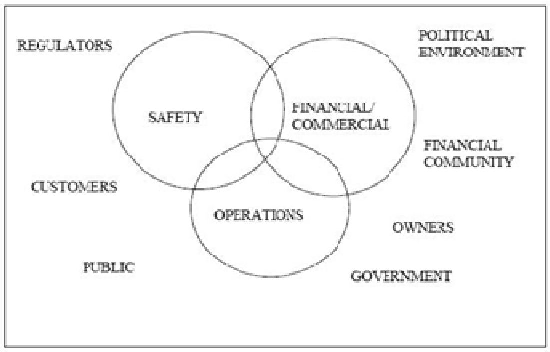

Figure 3: Risk Management Environment Outline

The safety sector covers power generation and its related risks as well as the general industrial safety and environmental risks posed by industrial activities. On the other hand, the financial realm covers matters like currency risks, product/resources pricing risks, pressure from competitors, insurance undertakings and requirements, price derivatives, debt interest rates, and capital market performance. Meanwhile, strategic risks touch on matters that affect all the three aforementioned issues including mergers and acquisitions, responses to privatization, and product/market diversification [13]. The proposed framework defines a systematic approach to the risk identification and mitigation cycle as described by the figure below.

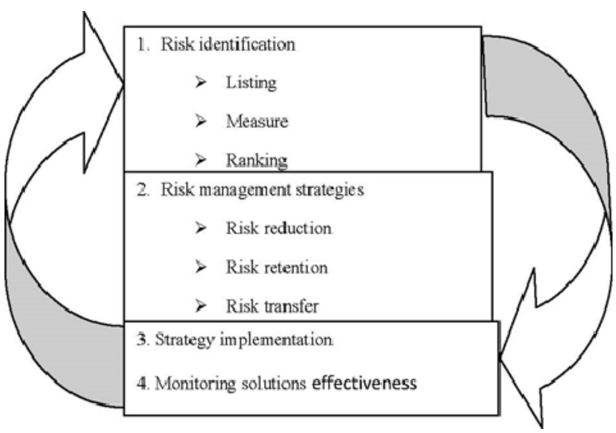

Figure 4: Risk management framework

The framework is founded on a methodology which ensures that all the possible consequences and mitigation strategies are adequately explored to ensure that adverse effects are minimized and the industries performance is maximized in a cost-efficient manner

Checklist for risk management framework application in power and automation industries: The risk management approach framework only applicable if a systematic approach is employed in its implementation, This is possible if the help of a checklist is employed in its implementation thereby creating room for documentation of emerging risk. The checklist prompts the sectors managers to critically analyse risks associated by the production process, management decision making, and financial implications to the firm. Though not exhaustive enough, the checklist initiates the thinking process associated with a particular risk. In general, the checklist helps in identification of risk consequences, ranking them according to importance, explore possible management techniques, cite issues involved in implementation and hence develop a monitoring and feedback system (See appendix 1-4: Risk management checklists). The checklist defines a four-step checking procedure, which ensures that all aspects of the aforementioned framework are adequately explored,

Risk Management Processes Identification, Measurement and Assessment of Risks: The sources of risks in power and automation industries are vast in nature. Such risk sources include processes of production and training, social responsibility, external influences (e.g., natural disasters and economic effects), and financial management) [10]. Identification of these sources can be done with the help of specific/generic risk checklist, developing critical processes flow charts, contract examination, engagement in physical inspection, financial statements analysis, and interviews with employees, contractors and regulators. Often advanced information systems are used in obtaining constant update on firm operations, asset acquisition, and the firm's relation to its external. Risk management processes generally ensure that unintentional/unconscious retention of risks does not occur due to undiscovered performance variability. Characterizing the already identified risk is an important process. Deterministic and probabilistic safety analysis is often employed in power and automation plants in management of safety risks. Their expansion could in-corporate measurement and assessment of risks associated with power and automation industry processes including plant investment protection, plant variability maintenance, and relicensing issues analysis. Qualitative questions can be used in helping power and automation industry managers to examine the important characteristics accompanying a risk based on a conceptual viewpoint. These questions include:

- Does the risk result in opportunities or risks?
- Is the risk cause episodic or a continuous thing likely to have continued effect?
- Can the risk source be reversed by a managerial decision-making?
- What potential effects are posed by the risk to the power and automation industry performance?
- Is the risk source mission critical or is it a source whose result modification is less severe?
- Does the risk affect production ability or does it just affect the way of production occurrence?
- Does the risk have financial effects?

However, it may be noted that note that not all the risks identified have negative effects on a firm's performance.

Financial analysts often argue that increased returns are subject to higher risk taking. Identification, measurement, and assessment take into consideration all the risks that a firm may incur regardless of their corresponding effects. To further understand the risk identification process, adequate discussion of each risk sector within the context of power and automation industries is important.

Safety related risks: In this context, safety-related risks are defined on the bass of key safety areas encountered within power and automation industries [14]. These include electrical and electronic, environmental risks, and industrial safety risks. In characterization of these risks, it is important to not only consider the types involved but also attempt to establish both the internal and external consequences associated with risk. Safety risks are extensively researched on and most of the industries have safety manuals within the plant premises. However, it is not enough to merely develop safety manual within the context of previous research. Every industry must independently audit its own safety vulnerabilities and hence develop appropriate manuals.

While electrical risks are generally physical and easy to analyse, with automation comes a new form of risk. Cyber risks pose new threats to control networks. Though typically well engineered, they are subjected to infringement and system crash. In building cyber safety, its asset's functionality must be critically assessed and their communication with each other must be established.. Corporate IT vulnerability assessments use both commercial and open source tools in analysis of cyber security states of the respective automated systems. Often, it is appropriate to run the tools in network test environments to avoid self-imposed denial of service attacks. This ensures that the effect is not transferred to the actual production environment. Virtualization technology offers an appropriate avenue for network emulation. However, it is important that the virtual system used is representative of the production environment with all un-patched services and system wholesomely running. Some of the vulnerable cyber assets employed in power and automation industries are summarized below

Vulnerable Cyber Asset	Description
Energy management system (EMS)	In AREVA e-terra habitat multiple high-risk vulnerabilities are identified
Historian	Authentication weakness of OSIsoft PI Server
Remote Telemetry Unit (RTU)	power pole RTU is Bluetooth accessible
Advanced Metering Infrastructure (AMI) / Smart Meter	Smarter grid-related vulnerabilities, more specifically AMI and smart household devices
Programmable Logic Controller (PLC)	Remote accessibility of Omron PLCs via apple iPhone Scada mobile application.

Operational Risks: Properly run power and automation plants provide impressive improvements with regard to production processes and hence reduced lengths of outages, reduced plant trips, reduced staffing levels, and improved management of discretionary projects. For deeper understanding, it is important to assess the sources of operating performance variations. Multiple unit power and automation power industries face additional challenges that occur concurrently including:

- Operation and relicensing of older plants which include life extension and management
- Performance improvement of operating plants
- High speed of implementing new plants in order to realize investment returns early enough.

Addressing these issues requires technological upgrades and innovativeness with regard to future challenges expectations. Though contributing significantly to increasing power needs, the management had to make decisions with regard to the future risks and implications which an expansion posed to the power plant. The skill-base requirement was also an important factor to consider in developing an effective risk analysis plan for such a scenario. Tightened skill market from engineers may at times require indigenously bred skills, which would require time to develop.

Operations are also affected by periodic safety upgrades to power and automation industries. While such upgrade are based on the assumption that they ultimately reduce the overall risks, accounting for other risk aspect may render its overall benefits less oblivious. Upgrades give rise to aspects of risks. Industrial safety risk is associated with the safety upgrade while operational risks arise from running of the plant alongside installation works. Attempting to fit new systems to plants, which did not earlier give room for such, may prove futile and challenging to the engineers. Such construction may bring with it severe injury risks far greater than normal power and automation power industries safety risks the system is expected to improve.

Financial risks: Just like any other business, power and automation industries are subject to financial risks. Prioritization is thus fundamental in safeguarding of stakeholders returns. Financial risks to power and automation industries are either internal or external. External risks are often beyond the industry's ability to rectify them. The industry is thus forced to adjust its operations as a risk management measure rather than to attempt to correct the external factor. Such risks include economic conditions, contractual risks, competition risks, and fuel costs among others. Internal risks, on the other hand, are financial risks, insurance and claims, threats posed by double running investments, increment in net debts and credit risks, and threat of legal actions. Unlike external risks, internal risks are a making of the industry. They usually result from managerial decisions made by the industry's management team. Such risks are within the control of the industry and hence the industry can undertake corrective measures.

Determination of Appropriate Risk Management Techniques. A combination of management techniques are often employed in evaluation of the best methods suited for the risk faced by power and automation industries [9]. The three aforementioned generic techniques are employed in risk management. These include risk reduction, retention of risk, and transfer of risk. In practice, a particular risk will be addressed using one of the methods. It is however important to evaluate whether a specific solution addresses the different areas of risk interaction. For instance, in implementing a power safety design change, it would be important to access whether the proposed solution might conflict with industrial safety regulations/procedures. Identifying appropriate risk management techniques therefore requires assessing of the interaction effects touching on a range of factors including safety, production procedures and operations, financial decisions and strategic decision making.

Risk reduction:. Risk reduction takes a two dimensional perspective: this includes reducing the likelihood or frequency of events occurrence and reduction of the consequences that an event is expected to have in case it takes place. Reduction of occurrence frequencies involves a range of techniques including engineering procedures, employee education programs, and standards enforcement. Severity reduction, on the other hand, includes barring events progression from less severe episodes to more severe episodes and employment measures which reduce economic impact of critical disruptions. Risks reduction measures may therefore involve pre-event measures, simultaneous measures that run in tandem with the events and post-event actions.

Transfer of Risk: Risk transfer involves obtaining a substitute to the original party exposed to risk. The substitute bears the risk on behalf of the original party . Such transfers are done through contracts and financial market instruments. The risk degree is at times reduced through transfer in instances where the party accepting the risk possesses portfolio effects, e.g. insurance contracts which involve pooling of risks. In some instances, the risk remains the same but is transferred to another party who is willing to accept the performance variability at a price. Contractual agreements are the most commonly used risk transfer mechanism within the power and automation industry. In contractual agreements, the risk is shoved to the party who is able to control risk results, prevent the risk, and manage it if it occurs or is best suited to absorb its impacts. The counter party is then liable to premiums for the risk transfer. Such mechanisms include hold-harmless agreements, financial and commodity markets hedging, lease agreements, late delivery penalties, warranties, and insurance contracts among others.

Multi-trigger insurance cover is an emerging risk transfer mechanism used in power and automation industries. It is a development of insurance industry in an effort to improve its ability to compete within the capital markets. Double trigger policy, for instance, allows two uncorrelated actions specified if occurring simultaneously to trigger a payment, e.g. explosion of steam line, damage by storm or compensation of workers risk.

Figure below illustrates some of the multi-trigger insurance policies.

Type of Company	Triggers	Purpose
Electric utility	• Rainfall inches over a specified time • $X maintenance expenses from given storm.	The insurer pays much-higher-than-normal expenses incurred in maintenance.
Columbia Energy (a Dulles, Virginia natural gas utility)	• Unknown triggers	The customer price volatility, in case of fuel adjustment costs resulting from rise in retail prices, is transferred to the insurance company.
Energy trading company in New Zealand	• Specific water current of given upstream in New Zealand vs. electricity spot price	Insurance company pays higher than the normal price for electricity purchase.
Electric utility	Breakdown of boiler vs. days in which temperature go beyond set threshold vs. electricity price above set strike price	Payment of the much-higher-than-normal-price for replacement electricity purchase

Table 1: Examples of Multi-Trigger Insurance Covers

Multi-trigger insurance associated costs are often lower compared to traditional insurance and derivative instruments. For instance, the derivative cost for a dual trigger policy is four to five times less the traditional insurance Generally, the lower the trigger correlation, the lesser the costs are.. They are just like other insurance policies, priced with regard to their occurrence probability

Retention of Risks:. Retention is perhaps the least familiar risk management technique in power and automation industries. This is given that such plants operate on a principle of keeping risks at negligible levels. The idea of deliberating on acceptable risk levels is unacceptable within the industry. However, financial risks with probability of high returns remain present within the industry. In addition, regardless of the efforts, some unintentional risks often bypasses risk management initiatives and the rational decision making process. Such risks are unintentionally or unconsciously retained within the industry. An example of some of the risks retained within the power industry include usage of a risk informed tolerance flaws in design of less restrictive pressure-temperature limits Another example is the continued usage of a turbo generator that is already known to have flaws. This is done in consideration of the likely costs associated with process disruption before the normal maintenance period, and likelihood of its complete failure if repair is attempted. In general, despite attempts by power and automation companies to avoid retaining of risks, circumstances arise where the existing options are limited and the risk has to be retained.

Implementation and monitoring of risk management initiatives: Upon identification of the best possible risk management initiatives, the industry undertakes implementation actions simultaneously with the monitoring process to establish its successes and failures [8]. Implementation may involve organizational management changes, which are expected to affect the cited risks at implementation integrative decision support through the employment of software applications. Normally though, insurance, financial, and physical risk databases are separated. Such endeavours are possible with the help of integrated risk management packages. Such software also assists in monitoring of the implementation procedure and the possible outcomes upon identification of emerging trends.

Conclusion: As earlier mentioned, the global power and automation industry needs to take into consideration various risk dimensions within its context. This paper attempts to discuss useful tools and processes that risk managers in power and automation industries might find important to look into. It elaborates the need for power and automation industry managers to undertake a broad and objective management of safety-related, strategic, financial and operational risks within individual firms rather that generalizing. The paper additionally has provided a broad range of examples upon which the risk managers may draw reference in relation to the risk they meet and hence draw appropriate measures to the risks within their context. The need to incorporate the use of software within risk management environment is adequately addressed, with its benefits clearly outlined. It is upon this foundation that this paper is able to make the recommendations below.

Recommendations: This paper, based on its risk assessment discussion, with the context of power and automation industries makes the following recommendations:

- All power and automation industries need to incorporate risk management in all their undertakings, ranging from minor to major changes in processes, structure and general operations of the industry.
- Risk managers must realize that the use of software in risk management is inevitable in the evolving world and therefore, they need to undertake training in this area to ensure they are up-to-date with emerging risk assessment technologies.
- Training of staff on risk management should be regularly undertaken as may be deemed appropriate.

Acknowledgement
Neelakshi Ganguly of St. Thomas' College of Engineering and Technology, Electrical Engineering Department for help in editing.

References:

1. Pradip Banerjee, 1995. An Operation Paradigm for Power System Security/Economy Trade off
2. Jorion, P., 1997. Value at risk: the new benchmark for controlling derivatives risk. McGraw Hill.
3. EPRI, 1997. Achieving an effective living maintenance process: a handbook to optimize the process and keep it that way, EPRI Report TR-108774
4. Schimmoller, B.K., 1999. Plant equipment adapts to changing market. Power Engineering
5. Pradip Banerjee, 2001. Electricity in 21st Century
6. Donde, S. and Fox, B., 2001. Risk management savvy vital under deregulation. Power Engineering 11,
7. Zink, J.C., 2001. Integration of probabilistic risk assessment in power plants. London: McGraw Hill.
8. Kurt, A. F., 2002, Risk-Based Analysis for Managers. London: McGraw Hill
9. Cris, W. et al., 2002. Interfacing the assessment, management, and communication of risk
10.Hengel, A., 2002. Effecting sound risk management practices. Risk Management Journal 2, (4): 62
11.Energy Regulatory Commission, 2006. An approach for plant-specific, risk-informed decision making: technical specifications (TS). Regulatory Guide 1.177
12. Berg, H.P., 2007. Approach for risk-based regulation and risk management of power plants. Consortium for Electric Reliability Technology Solutions (CERTS), N.D.
13.Fuhr, P., 2009, April. Wireless and the smart grid. InTech.
14. Greenfield, D., 2010. Connecting energy, cost, maintenance and process management ideas through a unique systems integration approach and energy harvesting potentials takes center stage at ABB's annual event. Design News 1, (2) 11.

AUTHOR

Pradip Banerjee

B.E. (Electrical Engineering), Gold Medalist, 1972. Worked for 42 years in Design & Project Engineering of Big Industries, particularly Thermal Power Plant). After retirement was involved for 3 Years in teaching in an Engineering College as Asst. Professor in Electrical Engineering Department.

Contact: pradipb1972@gmail.com

CO-AUTHORS

Anindita Banerjee, B.Tech. (Electrical Engineering), 2004 Worked in Consulting Engineering Organisation for 13 years in design engineering of Thermal Power Plant / Gas Turbine Plant in India and abroad. Afterward working in Turn-key Contracting Organisation of Extra High Voltage Substation / Transmission line Vertical as Manager Design.

Contact: aninditabanerjee1@gmail. com

Anindita Ganguly, ardent control system enthusiastic.

Contact: aninditaganguly80@gmail.com