Risk Management in Automation and Power Industries

Name:

Institution:

Date:

Table of Contents

Table of figures

List of tables

Executive summary

Power provides the basis on which the global economy runs. Modern power and automation technologies have seen greater advancement within the industrial scenario. Such advancement has seen the incorporation of flexible and smarter power and automation industrial technologies. For instance, operations that once depended on pneumatic manual controls decentralized across production channels are now central-based and controlled by advanced computerized system. The advanced technologies generally involve human-computer interaction systems that 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.

Automation is defined as a process of replacing traditionally human industrial functions, with machine elements that automatically make decisions and operate the system, e.g. use of robots (Berg, 2007, p.12). Automated power industries not only focus on production efficiency but also strive to strike a balance between production and consumption. 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 mitigation procedures.

However, this paper will go beyond mere security risks to access the possible risks faced by power and automation industries in their operations. Additionally, the paper will look at possible causes and mitigation measures available to such industries. Finally, the paper will provide policy suggestions for enhanced risk mitigation.

Introduction

Industry Landscape

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. 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.

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 (Berg, 2007, p. 47). 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 (Richardson, 2010, p. 4).

Many states are currently exercising increased roles in enhancing automation within power industries. Moreover, respective regional bodies have developed stringent compliance and regulatory guidelines including the Sarbanes Oxley Act (SOX), FERC and NERC regulations (North American Electric Reliability Commission) (US Energy Regulatory Commission, 2006, p.34). Additionally, state and public service commissions continuously make policy changes that increase challenges for power and automation industries risk managers. In North America, for instance, there is The North Electric reliability Corporation's (NERC) critical infrastructure protection (CIP) reliability standards which obliges industrial players to meet implementation deadlines or risk a heavy fine of up to $1 million daily for each non-compliant requirement (US Energy Regulatory Commission, 2006, p.41). However, such rigid compliance requirement has proven onerous to the industrial players, hence giving rise to legal risks by the players.

Over the years, states have ceded ownership of power and automation firms to the private sector. This move is aimed at encouraging competition, cost reduction, and reducing government's engineering workload. Most firms are now focusing on beating shareholder targets rather than government goals. This has opened the market to an array of risks as a result of deregulation. 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 (Donde and Fox, 2001, p.13). 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.

For purposes of this paper, risks to power and automation industries will be classified as safety, operational, strategic, and financial risks. In a research conducted by the Institute of

Nuclear Power, it was established that the categories aforementioned exhibit a correlation noting that increased safety results into a corresponding increased strength in the firm's economic performance (Institute of Nuclear Power, 1995, p.12). The research 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 (Cris *et al*, 2002, p. 2):

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

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).

Figure 1: 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 suceptibility to commercial and security threats resulting from inconvertibility/transfer restrictions of currencies, contract breaches, confiscation/nationalization threats (creeping expropriation of assests), and wars/civil unrests (Hengel, 2002, p.62). 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 realtime data availability. Discrimination between the varying threats and hence their relative importance remains a great challenge to the risk managers in power plants and industries. 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 assests and undertanding the weaknesses, expected losses, and appropriate tactics in mitigating the risks to ensure sustained values. The IEEE standard 15408 defines a common criteria risk assesment table that assists in depicting relationship of owners value to firm assests with respect to possible risks (Hengel, 2002, p.62) (see figure on the next page).

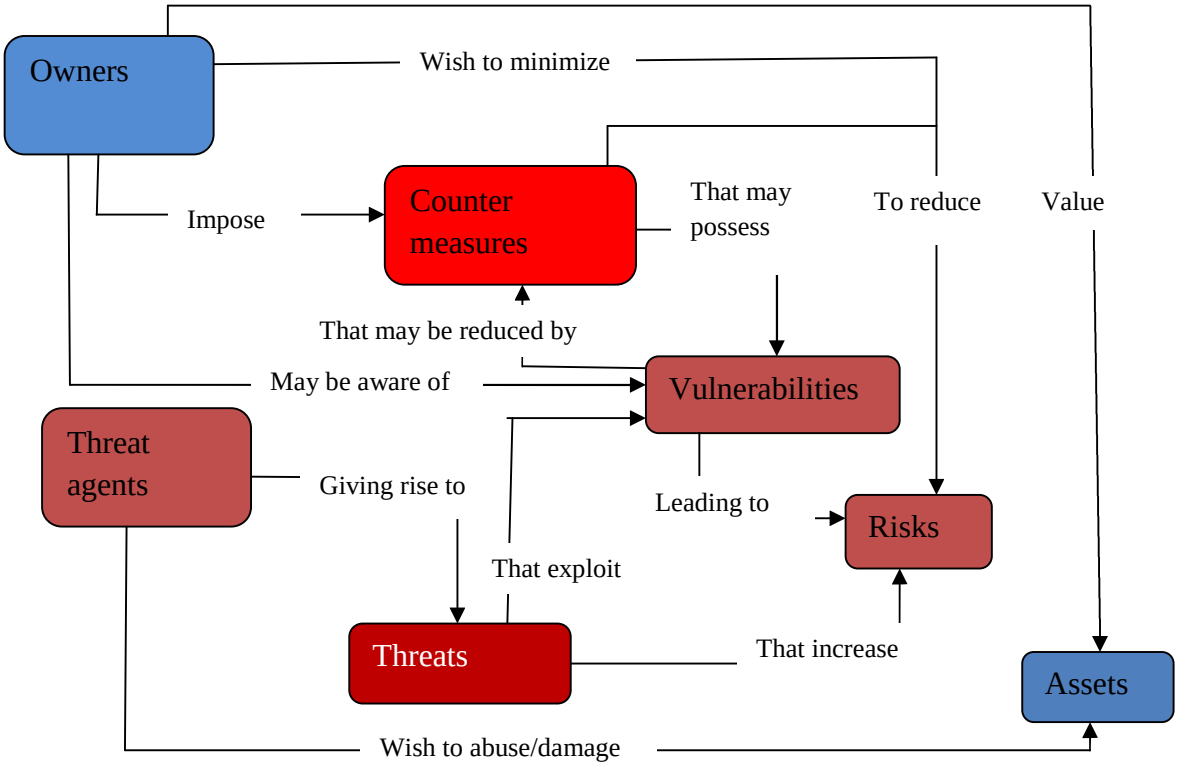

Figure 2: Threat reduction flow chart

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 (Robert, 1989, p.483). 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 (Robert, 1989, p.484). 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 (Richardson, 2010, p. 7).

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.

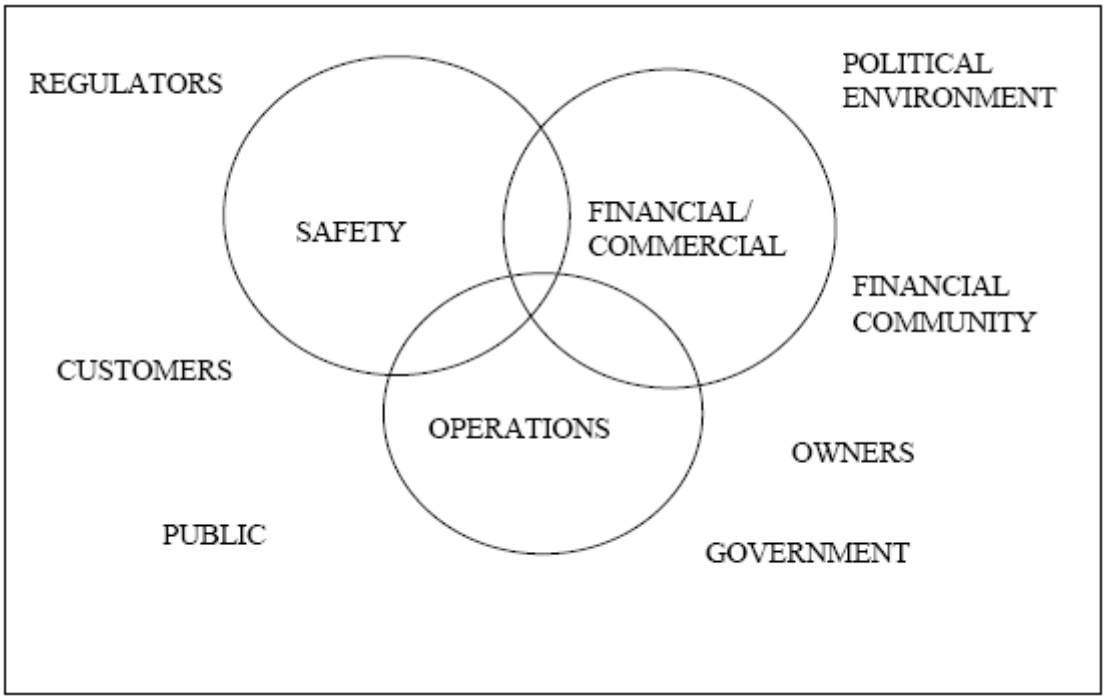

Figure 3: Risk Management Environment Outline

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 (Fuhr, 2009). The proposed framework defines a systematic approach to the risk identification and mitigation cycle as described by the figure on the next page.

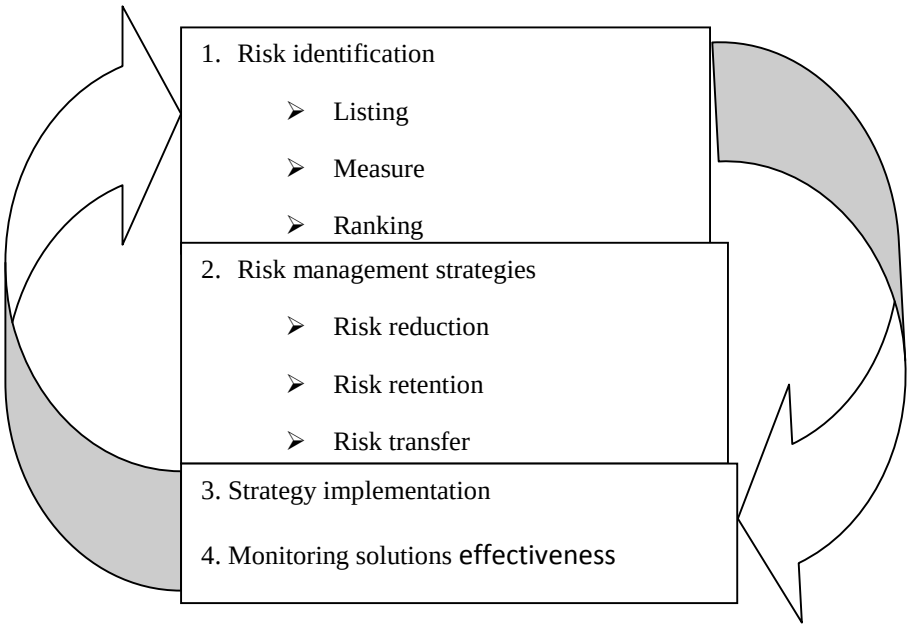

Figure 4: Risk management framework

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 (Fuhr, 2009). 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 analyze 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 (Luallen, 2009, p. 12). 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 (Luallen, 2009, p.34). 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 (Zink, 2001, p.18). 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 view point. 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, 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. 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 analyze, 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. NERC, from instance, developed a document for identification of cyber critical assets within a given system. 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.

OLE for Process Control (OPC)	MatrikonOPC is dependent on Microsoft Windows' object linking and embedding
Human Machine Interface	Buffer overflow of CitectSCADA
	Digital camera results in a plant shut down initiated by Indian Point Power.
Industrial Communications Hardware	A bridge default settings of Rockwell Automation ControlLogix 1756-ENBT/
	Stack overflow displayed by ABB Process Communication Unit 400
All	Communication of critical hardware across Ethernet I soften restricted by flooded communications
All	Risks of insider/partner risks where the IT contractors turn against the employer
Several (traditional corporate cyber assets)	Vulnerabilities to commercial applications and platforms like Linux, Unix, AIX, Windows, etc.
	Addition of assets/communication channels and changes non-documentation.
	In appropriate default services and default, administration and sharing of user accounts
	Spanning of control and cooperate networks by multi-homed devices

The table above represented some of the key vulnerabilities that accompany automation. More vulnerabilities are discovered by the days as unscrupulous individuals attempt to infringe such systems either for malicious or adventure purposes. The real challenge is in assessment of immediate configurations of IEDs, e.g. remote terminal units (RTU), PLCs, relays and other devices used in network controls (CERTS). This calls for incorporation of cyber security professionals in understanding of utility specific devices configuration. Mostly, limiting of

system vulnerabilities relies on system firmware and constant software updates. Updates are confirmed via integrity checks like SHA (2)-256 among others (CERTS).

Industrial, environmental and electrical safety assessments are supplemented by both national and international guidelines which act as the reference standards upon which safety assessment is based. Arguably, safety assessment tools in power industries remain one of the best developed ones as compared to other industries. Each industry has additionally developed internal frameworks for management of environmental hazards. British energy, US for instance, has a framework that makes it mandatory for all power and automation industries to avail inventory of potential environmental hazards from its operations and their respective magnitudes (Luallen, 2009, p.11). This framework provides a point of integrity and barriers aimed at ensuring hazard free/minimized environment. This informed risk analysis approach allows room for focusing resources on most beneficial trend to all stakeholders as risk is all round. Additionally, in 1998 USNRC undertook a major regulatory sweep, shifting away from the traditional resource intensive, subjective and arbitrary compliance errors analysis to more objective, measurable, safety significant indicators of performance (Institute of Nuclear Power, 1995, p.34). Its focus then moved toward process/system inspection and enforcement procedures based on aforementioned indicators. Technical safety-related risks have additionally employed the use of PSA methodologies with regard to their nature and impact to technical specifications. Accepted TS approach is based on traditional engineering evaluations procedures in analysis of significance of risks in the proposed changes (US Energy Regulatory Commission, 2006, p.18).

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 instance, EPRI document described the best approaches to typical plant maintenance procedures. The document focused on safety and maximization and cost minimization. For deeper understanding, it is important to assess the sources of operating performance variations.

PSA methodologies are used in allocation of in-service inspection of resources in a cost-effective way. Application of PSA allows power and automation plants to reduce the scope of examination of the existing ISI programs by $\sim 60 - 80\%$ (Institute of Nuclear Power, 1995, p.41). This significantly contributes to cost reduction and hence saving. Westinghouse's Science and Technology Center has developed a chaos theory methodology which undertakes deviating conditions in machinery (Institute of Nuclear Power, 1995, p.54). The methodology uses a model-based approach that brings together special adaptive filtering, together with tools for chaos analysis in discrimination of different, progressive fault modes with a system/process (Luallen, 2009, p.13). The goal of this theory is ensuring that major maintenance activities like bearing changes and turbine balancing are only conducted when appropriate.

Operational risks may also result from acts of God and damage to property. Power and automation industry operators need to design, systems, structures and components (SSC) which can withstand the effects of natural disasters, including floods and earthquakes. While in the past testing was reliant on expensive specialized services and laboratory procedures, modern techniques incorporate the use of computer models that test SSC integrity (Luallen, 2009, p. 21). These methods have significantly reduced the costs associated with such tests previously. For instance, Entergy Operations Inc. in Arkansas is located in a tornado prone area; the plant uses large external emergency condensate storage tanks as their source for emergency feed-water systems in case of main feed-water system failure (Greenfield, 2010, p.17). This is a risk

management strategy employed by these nuclear power plants. When a necessity to modify tank design and protection system arose, the engineers in the firm employed the use of Algor's Accupak/VE Mechanical Event Simulation software in recreation of tornado events, motions and consequences which include inertial effects, impact projections, permanent deformations and effect of residual stresses (Greenfield, 2010, p.17). This software serves as an example of simulation software that have enhanced risk management procedures and testing to the context of the expected threats.

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. In Entergy Operations Inc. for instance, the initial plan was generation of 220MWe PHWRs but later increased potential of up to 500MWe PHWRs was identified (Consortium for Electric Reliability Technology Solutions, n.d.). 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 (Schimmoller, 1999, p.15). 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.

Financial risks are a product of financial variables that are affected by various undertakings of a power industry. Analysis of financial risks include a deeper examination of resources pricing, power pricing, new ventures costs, probable losses from a unit failure in multi-unit operating industries, contractual related losses, fluctuations in currency in circumstances where multi-national transactions take place (Schimmoller, 1999, p.15). The risks may be classified as financial market risks, credit risks, liquidity risks, and financial operations risks.

Value at risk methodology has emerged as a state-of-the-art way of measuring financial risk within an enterprise. It summarizes the maximum loss expected over a target horizon at a specified confidence interval (Jorion, 1997, p.16). Its calculations are based on standard statistical methodologies. It helps apprise the senior management team on the risks involved in its trading and investment undertakings inform the shareholders and financial markets on the financial risks and hence, enhance better debt pricing, create a comparison of risky market activities, adjust risk performance measures and improved cash flow management in multiple currency trading (Jorion, 1997, p.16).

Internal financial risks pose a major risk to all industrial players—the most recent being the economic recession awakened all industries, power and automation industries inclusive to a reality of the external financial effects to company's financial performance. The energy information in the United States reported industrial energy consumption as being the largest compared to all the other sectors. This makes the overall industrial sector a major client to the power and automation industries. The effect of economic recession on this sector led to a decline in energy consumption. For instance in the US, industrial consumption decline from 33% of total national grid in 1996 to 25% in 2009 (U.S. Energy Information Administration, n.d.). This comes with a decline in income generation by the power and automation industries. Such a decline

negatively affects industrial performance and it has to devise ways of managing this risk, either through cost cuts, discontinuing some of its operations or in some instances, through debt outsourcing. Debt outsourcing, on the other hand, increases the net debt owed by the industry, which is not a good sign for its growth. Additionally, it results in a reduction in free cash flow thereby limiting investment undertakings that the firm may engage in.

Credit risks are caused by the downgrade of a borrower's credit rating hence market value decline. It arises from unwillingness of counter-parties to fulfill their contractual obligations. The credit risk level is estimated through calculation of the costs incurred in replacing cash flows in case of defaulting by the other parties. It includes imposition of foreign exchange restrictions by the domicile countries; hence the counter-parties find it difficult to honor their contractual obligations. Power and automation industries also suffer liquidity risks in instances where transactions cannot be undertaken within prevailing environments due to market activity insufficiency and inability to meet the flow of cash obligations. For instance, the economic recession created an environment where consumer had to reduce production and hence reduced power requirements (U.S. Energy Information Administration, n.d.). This threatened the income generation and hence cash flow of various power and automation industries in Europe and the United States (U.S. Energy Information Administration, n.d.). Financial operation risks result from model misspecifications, system inadequacies, failures in management, faulty controls, fraud, and human errors in financial resources management.

Financial market risks are a result of market price changes with regard to assets and liabilities leading to absolute risks (a measure of potential loss in currency values and often results into volatility to total returns), relative risk (comparable to benchmark indices), and basis risks (result from breakdown of relationship between products used in hedging each other or are

non-linear). A change in currency value during an accounting period of multinational firms, which engage in cross-boarder transactions with buyers and suppliers, is likely to either negatively or positively affect the industry. Most multinational companies often attempt to manage these risks by putting in place measures that cushion it from such.

The recent commodity prices increase is creating increased concern among the industry's players. The strained materials market is a product of increased global demand at the pre-recession period. The industry's management have to think more strategically in their product design to avoid unaffordable rates to consumers while at the same time profitably produce. Most cited pricing increases that are causing concern within the power industry is the increase in copper and aluminum pricing. The emerging tradeoff of material cost and energy efficiency maximization remain key driving forces in the power and automation industry. Some power industries are already exploring the possibility of having a complete shift to use of thermoplastics given their pricing, light-end products, and recyclability as a risk management measure.

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. The three aforementioned generic techniques are employed in risk management. These include risk reduction, retention of risk, and transfer of risk (Richardson, 2010, p.23). 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 (Richardson, 2010, p.23). 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 (Zink, 2001, p. 17).

The other dimension involves increased understanding of the reduction and control tools and hence characterizes them in accordance with their focus on involved individuals behavior or the surrounding environment in which the physical assets and control system function. The common generic risk reduction techniques comprise of asset duplication and separation, salvaging techniques, system redundancies, subcontracting, leases, harmless hold agreements, and actions of indemnity (Robert, 1989, p.485). Such actions aim to reduce uncertainty and hence, increase certainty, alter high probability occurrences to low probability occurrences, improve system quality and thus reduce failure likelihood, enhance personnel training, reduce risk exposures by individuals, promote use of well-defined and documented

techniques/procedures, and encourage use of peer-reviewed processes, techniques and procedures (Robert, 1989, p.486).

Usage of smart instruments in power and automation industries is known to allow remote diagnostic capabilities which allow operators, industry management, and external experts to monitor equipment condition (Donde and Fox, 2001, p.91). For instance, such systems may easily identify imminent valve failures, faulty meter readings, monitor valve seat pressures, and report general abnormalities in a given process. Such information help in identifying system areas that need overhauling in addition to offering integrated information which assist in the development of preventive maintenance programs and hence, optimal personnel/resources utilization.

Component inspection is also an important tool in risk reduction in power and automation plans. It is an aspect of inventory management that allows downtime reduction as a result of installed components failure. Database software is used in inspection and repair data organization in addition to provision of budgetary information that enhance outage planning and management of components (Donde and Fox, 2001, p. 91). Such software is a powerful tool applicable to multiple power station industries and provides the appropriate mechanism for reducing the frequency with which more than one power station may be off-line as a result of failure of a component (Zink, 2001, p.24). An example of such software is the Component Assessment Management Software (CAMS). Other software applicable in management of risks include the monitoring and diagnostics software, combines data into intelligence and hence, helps reduce the magnitude and volatility associated with maintenance costs through provision of information on the best timing for maintenance operations, e.g. electric motor PDM, document management systems which assist in recording of the industry's configuration, processes and

procedures. Such a system reduces the costs incurred by the industry and likewise time. The risk of delay or loss in production is hence minimized in addition to ease in records and operating procedures change. CIMAGE document management systems used in the UK facilitates licensing, personnel training, safety regulation and document maintenance/retrieval (Garwatoski, 1999, p.11).

Power and automation companies are increasingly faced with competition pressure to keep plants in line and minimize outages. Reducing outages requires least variability in financial performance. Careful planning of logistics for staging and laydown of parts and equipment on asset space is vital. A proper and appropriate arrangement of parts is essential in any power and automation industry. Likewise, shift arrangement should be in such a way that efficiency is at maximum. Garwatoski (1999, p.14) asserts that careful planning and coordination can result in up to 15-day reduction of typical generator rewind cycle.

Cyber risk, on the other hand, is reduced through building of security walls to guard the system against invasion. Preventing man-made attacks require strong electronic security parameters and cyber configurations within the control systems. Commonly used resources include the NIST's Special Publication 800-82 v2, 18 Industrial Control Systems Security and the Cyber Security Procurement Language for Control Systems (Department of Homeland Security). A combination of computing cyber environment under internal networks controlled by a single authority/policy is used to reduce security threats significantly.

In general, risk reduction is a common practice in power and automation industries in their focus to enhance efficiency while, at the same time, keep risks at minimal levels.

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 (Robert, 1989, p.482). 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.

Insurance contracts allow power and automation industry operators to get compensation for losses they incur within the contract definition. Insurance policies applicable to power and automation industries include public liability, employee liability, damage/broken material, and loss of output/sales compensation (Donde and Fox, 2001, p. 96). Financial derivatives like hedging of risks are also used to transfer risks as a call option. Such agreements give the buyer a right to purchase a product at a given price. In instances where the market prices exceed the call prices, the buyer is allowed to get the commodity at a price lower than the market price. Swap contracts are also used in risk transfer. It involves scenarios where the counter party faces an opposite type of problem (Donde and Fox, 2001, p.101). For instance, a swap contract may be applied to protect against revenue losses as a result of a warmer-than-expected winter.

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 (Zink, 2001, p.40). This method provides a competitive advantage to power plant operators as they use to hedge risks in the world markets producing electricity. 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.

Table 1: Examples of Multi-Trigger Insurance Covers

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

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 (EPRI, 1997, p. 6). Generally, the lower the trigger correlation, the lesser the costs are (EPRI, 1997, p. 6). 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 still remain present within the industry. In addition, regardless of the efforts, some unintentional risks often by-passes 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 (EPRI, 1997, p.10). EPRI study, for instance, revealed a possibility of increasing allowable pressure by up to 50Psi without increasing vessel failure risk (EPRI, 1997, p.9). 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. 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 endeavors 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.

Conclusions and Recommendations

Conclusion

As earlier mentioned, the global power and automation industry needs to take into consideration various risk dimensions within its context. This report attempted 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 report 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 report is able to make the recommendations below.

Recommendations

This report, 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.

Appendices

Appendix 1: Risk Identification Checklist

Step 1: Identification of Related Risks				
Category/description	**Definition**	**Opportunity/Threat**	**Measurement units**	**Rankings**
SAFETY RELATED				
Environmental				
Electrical and electronic				
Industrial				
(Others……)				
OPERATIONAL RISKS				
Qualification of personnel				
Training of personnel				
Outage Management				
Management of inventory				
Documentation and Procedures				
Structure of the organization				
Physical Security				
Human Factors				
Aging effects				
(Others …..)				
FINANCIAL RISKS				
Interest Rates				
Currency Exchange Rates				
Supply/Demand Conditions				
Flow of cash				
Investment returns				

(*Others…..)*				
STRATEGIC				
Political Environment				
Ownership trends				
Competition level				
Public image				
Legal environment and regulatory bodies				

Appendix 2: Risk Management Strategies/Techniques

Step 2: Identification of techniques/strategies best suited to manage the risk	
Risk reduction	**Identification**
Changes in engineering practices	
General organizational changes	
Existing standards enforcement	
Changes in personnel e.g. staffing/training	
Cost changes included enhanced efficiency, spending changes e.t.c.	
(*Others…..)*	
Transfer Risk	
Entering into contracts	
Insurance covers	
Regulation/Legislation	
(Others……)	
Retain Risk	
By Choice	
By Default	
Not Recognized	

Appendix 3: Solutions Implementation

Step 3: Solutions being implemented	
Solution	**Comments**
Assignation of responsibilities and accountabilities	
Employing sanity checks as to whether the solution works or not?	
Checking the consistency of the solution	
Are key risks being addressed?	
Possibility of an exit strategy	
Maintenance of flexibility	
(*Others…..)*	

Appendix 4: Monitoring Implementation

Step 4: Monitor Effectiveness of Solutions being implemented	
Action	**Remarks**
Establishment of success measures	
Analysis of Milestones and Check Points	
Unintended Consequence's identification	
Accountability monitor	
Emerging Risks monitoring	
Feed backs/adjustment possibilities	
Exit	

References

Berg, H.P., 2007. *Approach for risk-based regulation and risk management of power plants*. The 1996 Annual Meeting of the Society for Risk Analysis—Europe.

Consortium for Electric Reliability Technology Solutions (CERTS), n.d. [online] Available at <http://certs.lbl.gov/certs.html>

Cris, W. et al., 2002. Interfacing the assessment, management, and communication of risk. In Kurt, A. F., 2002, *Risk-Based Analysis for Managers.* London: McGraw Hill.

Donde, S. and Fox, B., 2001. Risk management savvy vital under deregulation. *Power Engineering* 11, (2) 11-15.

EPRI, 1997. Achieving an effective living maintenance process: a handbook to optimize the process and keep it that way, *EPRI Report* TR-108774.

Garwatoski, F., 1999. *How to cut rewind times by 15 days or more.* London: Modern Power Systems.

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.

Hengel, A., 2002. Effecting sound risk management practices. *Risk Management Journal* 2, (4): 62.

Institute of Nuclear Power, 1995. Perceived nuclear risk, organizational commitment, and appraisals of management: a study of nuclear power plant personnel. *Risk Analysis Report.*

Jorion, P., 1997. Value at risk: the new benchmark for controlling derivatives risk. McGraw Hill.

Luallen, M., 2009. *Securing a smarter grid: risk management in power utility networks.* New York: NitroSecurity.

Pool, R., 2002. When failure is not an option. *Technology Review* 11, (2) 42.

Richardson, J., 2010. *Fundamentals of risk management*. London: International Faculty of Finance.

Robert, E.R., 1989. The inside counsel movement: professional judgment and organizational representation. *IND. L.J.* 64, 479, 481-86.

Schimmoller, B.K., 1999. Plant equipment adapts to changing market. *Power Engineering* 4, (3) 11 – 23.

U.S. Energy Information Administration, n.d. [online] Available at <www.eia.doe.gov>

US Energy Regulatory Commission, 2006. An approach for plant-specific, risk-informed decision making: technical specifications (TS). *Regulatory Guide* 1.177.

Fuhr, P., 2009, April. Wireless and the smart grid. *InTech.* [online] Available at <www.isa.org/intech/200904web>

Zink, J.C., 2001. Integration of probabilistic risk assessment in power plants. London: McGraw Hill.