ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications

Varun Kumar Tambi[1*], Nishan Singh[2]

Vice President (Software Engineer, Product Manager), JPMorgan Chase & Co. United States of America[1*]

Consultant, EXL SERVICE COM INDIA PVT LTD, India[2]

ABSTRACT: Traditional project risk management techniques are becoming less and less effective in the age of Industry 4.0, which is defined by sophisticated automation, data interchange, and cyber-physical systems. The practical effects of incorporating Industry 4.0 technology into project risk management frameworks are examined in this research. It suggests a new framework that improves risk detection, assessment, and mitigation techniques by utilising technology like artificial intelligence (AI), big data analytics, and the Internet of Things (IoT). This paper illustrates how Industry 4.0 is revolutionising risk management procedures by looking at actual case studies and industry implementations. The framework offers practical insights for practitioners looking to adjust to the changing technological landscape by addressing important possibilities and obstacles. The findings suggest that incorporating Industry 4.0 technologies can significantly improve risk management efficiency and project outcomes, offering a pathway for organizations to navigate the complexities of modern project environments.

KEYWORDS*:* Risk Management, AI, IoT, Data analytics, Industry 4.0

I. INTRODUCTION

The rapid evolution of technology heralded by Industry 4.0 has fundamentally transformed the landscape of project management, presenting both unprecedented opportunities and complex challenges. As organizations increasingly adopt advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data analytics, and cyber-physical systems, the traditional approaches to project risk management are becoming insufficient to address the dynamic and interconnected nature of modern projects. Industry 4.0 technologies offer powerful tools that can enhance risk identification, assessment, and mitigation, but they also introduce new types of risks and uncertainties that must be managed effectively. This paradigm shift necessitates the development of a robust and adaptive project risk management framework that is capable of leveraging these technological advancements to improve decision-making and project outcomes. This paper delves into the practical implications of integrating Industry 4.0 technologies into project risk management practices, aiming to develop a comprehensive framework that addresses the unique challenges posed by these technologies. By analyzing the intersection of Industry 4.0 innovations and risk management principles, this study provides valuable insights into how organizations can harness these technologies to proactively manage risks, optimize project performance, and achieve strategic objectives. The research underscores the need for a paradigm shift in risk management approaches, offering a forward-looking perspective on how emerging technologies can be systematically incorporated to enhance the resilience and effectiveness of project management in the era of digital transformation.

Industry 4.0 represents a significant advancement in manufacturing, characterized by the integration of all machine components through interconnected data chains and operations. Originating from Germany with the idea of merging the Internet with manufacturing processes, this new industrial revolution builds upon the previous era's focus on electronics and information technology. Unlike earlier phases, Industry 4.0 emphasizes connecting production sub-components through the Internet of Things (IoT). The term "Industry 4.0" was first introduced at the Hanover Fair in 2011 and

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

encompasses a range of technologies and concepts including Cyber-Physical Systems (CPS), the Internet of Things, Internet of Services, Internet of People (IoP), and Internet of Energy.

A survey of over 2,000 companies reveals a strong expectation for a substantial increase in digitalization across industries. This transition is anticipated to result in the emergence of digital enterprises where physical products are enhanced with digital interfaces and data-driven services. These enterprises will collaborate within digital ecosystems involving both customers and suppliers.

As this industrial transformation unfolds, new risks will probably arise, potentially impacting various aspects of companies' operations. This suggests a pressing need to develop and test new risk management approaches tailored to Industry 4.0. The integration of IT and digital infrastructure in manufacturing introduces new potential hazards. Risks from the IT realm, such as cyber-attacks, malware, spyware, data integrity issues, and information availability problems, may threaten the industrial manufacturing process. Additionally, technical documentation and specifications may become targets for hackers and software pirates, further underscoring the need for robust risk management strategies in this new era of digital manufacturing.

Sustainability in production has long been a goal for companies, with one of its most notable milestones being the development of the Toyota Production System (TPS) in Japan. The drive for sustainability has pushed manufacturers to produce high-quality products while minimizing defects. This approach aligns with a deeper understanding of customer needs and the efficient use of resources, including raw materials, labor, and machinery. As a result, numerous studies have shown improvements such as reduced production cycle times, increased machine availability, optimized costs, and layout improvements, which contribute to lower inventory levels, reduced lead times, and minimized waste. The advancement of technology has further accelerated the global adoption of TPS by providing valuable data insights. This data enables the uncovering of hidden information and supports better decision-making. With the rise of Industry 4.0, customer expectations have evolved to demand greater production transparency and traceability. These requirements necessitate digital transformation and significant investment from companies but offer opportunities for process improvements and more strategic production scheduling, enhancing resource management. This article aims to present a method for integrating reliability considerations into the planning phase of production, which is crucial for negotiating with customers and finalizing contracts. By addressing reliability in the planning stage, companies can enhance their reputation and avoid potential penalties. The case study included demonstrates the practical application of this approach through workshop layout and small-batch project scheduling. It shows how a modified stochastic method can support factory scheduling, considering both scenarios where inventory costs are significant and where they are not.

Industry 4.0

Industry 4.0 represents a significant transformation in industrial processes, characterized by the integration of Internet of Things (IoT) technologies into industrial operations. This shift enables real-time digital connectivity across company boundaries, facilitating seamless horizontal and vertical integration of people, machines, objects, and information systems to dynamically manage complex systems.

The concept of Industry 4.0 encompasses a real-time, intelligent network that connects various elements of the production process. Despite its broad definition, interpretations of Industry 4.0 vary across research disciplines, each emphasizing different aspects of the concept. Central to Industry 4.0 are Cyber-Physical Systems (CPS), which integrate sensors, data processors, and actuators to merge the physical and virtual worlds. These systems allow for the real-time exchange of data between people and objects throughout the value chain.

Triple Bottom Line of Sustainability

Recent awareness of the environmental impacts of industrial activities has grown, particularly since the publication of the “Brundtland Report” by the World Commission on Environment and Development. This heightened awareness has shifted corporate philosophies away from a sole focus on maximizing profits to a more inclusive approach that

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

considers the interests of all stakeholders. This change has bolstered the importance of Corporate Social Responsibility (CSR).

The Triple Bottom Line framework of sustainability encompasses three key dimensions: profit, planet, and people. These dimensions reflect the economic, environmental, and social aspects of sustainability. Economic success is crucial for a company's profitability and financial stability, ensuring its survival. From an ecological standpoint, sustainability is achieved by using renewable resources and producing emissions that can be absorbed by the natural environment. The social dimension involves economic practices that respect and enhance human and social capital, completing the Triple Bottom Line. Given the interconnected nature of these economic, environmental, and social dimensions, it is essential to consider all three aspects when implementing Industry 4.0 strategies. Integrating these dimensions into strategic and organizational planning helps ensure that sustainability goals are met comprehensively.

Risk Management

The concept of "risk" remains ambiguous and varies widely in definition, reflecting its multifaceted nature. Many attempts have been made to define it, which underscores its complexity. For instance, Deloach describes risk as the degree of exposure to uncertainties that a company must understand and manage to achieve its strategic objectives and create value. March and Shapira, drawing from classical decision theory, define risk as the distribution of possible outcomes, their probabilities, and their subjective values. Miller, on the other hand, points out that "risk" often refers to factors that impact a firm's risk profile, such as "political risk" or "competitive risk."

The lack of a universal definition of risk can hinder communication and collaboration among researchers and practitioners. To improve understanding, this work adopts a prevalent classification that defines risks as measurable and objective, which allows for quantitative analysis. This definition views risk as the combination of uncertainty and potential damage.

In the business world, risk and uncertainty affect every process and decision, leading to potential errors, misjudgments, or unexpected changes with varied consequences for a company. Risks extend beyond individual firms to affect entire ecosystems, creating interdependencies among suppliers, customers, competitors, and the company itself. This complexity is further increased by digital advancements such as Cyber-Physical Systems (CPS), IoT, and Cloud Computing, which are part of the Industry 4.0 or Industrial Internet of Things (IIoT) framework.

Effective risk management aims to identify, analyze, and address potential threats. This process involves four key steps: identification, assessment, mitigation, and monitoring. These steps can be represented as a linear sequence or as a continuous cycle. This work extends traditional risk management by emphasizing a cross-company approach to identify and mitigate risks not only within a single organization but also across the broader business ecosystem.

II. LITERATURE REVIEW

Suraj Rane (2019) The aim of this paper is threefold: to identify the risks associated with construction projects through a literature review, to develop a project risk management (PRM) framework incorporating Industry 4.0 technologies, and to illustrate this framework using Internet of Things (IoT) technology. The study conducted an extensive literature review to pinpoint various risks related to construction projects. Based on these findings, a PRM framework utilizing Industry 4.0 technologies was crafted to enhance the effectiveness and efficiency of risk management. The framework was then demonstrated using IoT technology to monitor heavy equipment and related parameters. The paper showcases how Industry 4.0 technologies can be integrated into different stages of PRM. The literature review identified 21 specific risks associated with construction projects. Through the application of the PRM framework, it was found that sudden equipment breakdowns and equipment uncertainty are critical risks linked to heavy machinery used in construction. The complexity and specific features of individual projects may introduce additional risks that are not covered by the framework. The PRM framework leveraging Industry 4.0 technologies is designed to improve project success rates by enhancing the efficiency and effectiveness of risk management practices. The framework developed in this study offers a valuable approach for managing risks in construction projects. The use of IoT technology to demonstrate the framework provides a practical method for addressing risks associated with heavy equipment.

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

Hendrik S. Birkel (2019) The concept of "Industry 4.0" promises significant benefits for industrial value creation, but its implementation is hindered by various risks that are not fully understood. To address this gap, the paper proposes a risk framework specific to Industry 4.0, incorporating the Triple Bottom Line of sustainability—economic, ecological, and social dimensions. This framework was developed through a literature review and 14 detailed expert interviews. From an economic standpoint, the framework highlights risks such as high or misdirected investments, potential disruptions to established business models, and increased competition from new market entrants. Ecologically, it addresses issues like heightened waste and energy consumption and potential environmental risks linked to the "lot size one" production model. Social risks include job losses, challenges related to organizational change and employee retraining, and internal resistance to transformation. Technical risks are also examined, including challenges with technical integration, IT-related concerns such as data security, and legal and political uncertainties, like unresolved issues regarding data ownership. The paper concludes by discussing the framework in the context of existing literature, suggesting managerial and theoretical implications, and proposing directions for future research.

In the first scenario, aiming to minimize inventory costs, production was delayed until the latest possible time, allowing workshops more time to complete prior tasks. In the second scenario, where cost was not a factor, production began on the first day in each workshop and was completed before the deadline. These scenarios represent optimal solutions, but decision-makers can also explore alternative solutions based on the results. The modified stochastic critical path method highlighted production deficiencies, contributing to continuous improvement and better project time estimations. In recent years, manufacturing companies have focused on optimizing their resources to meet customer demands efficiently. Industry 4.0 technologies, such as Manufacturing Execution Systems (MES), support this goal by monitoring and controlling production through data collection and analysis. This article introduces a framework for implementing a risk-adjusted production schedule in a data-intensive environment. The framework uses production data from multiple workshops, which is analyzed statistically and applied in stochastic network models. The results of these simulations are used to develop a production scheduling model that allocates tasks among workshops.

Effective project management is crucial for successful operations and process management. This article explores the relationship between project success and specific components of Industry 4.0. Traditionally, project success has been evaluated reactively through cost, timeliness, and quality metrics. However, there is a need for more predictive indicators of success. To address this, a survey was conducted with 370 professionals in the digital technology sector. The survey included 55 questions covering 109 features, and the data was analyzed using various statistical methods. The results indicate that Industry 4.0 components could serve as effective predictors of project success, particularly in digital upgrades and improvements. These components are essential for ensuring effective and successful project management.

III. METHODOLOGY

The methodology employed in this study is designed to provide a comprehensive framework for understanding and managing risks in the context of Industry 4.0, with a focus on integrating cross-company perspectives. The approach begins with a thorough literature review to identify existing definitions and classifications of risk, providing a foundation for the study. This review highlights the multifaceted nature of risk and the various ways it has been conceptualized in different research disciplines. Building on this, the study adopts a quantitative approach to define risks as measurable and objective factors, allowing for numerical analysis. The methodology involves four primary steps: identification, assessment, mitigation, and monitoring of risks.

Initially, the identification phase involves recognizing potential risks that could impact both individual companies and their broader business ecosystems. This is achieved through a combination of expert interviews, surveys, and data analysis to gather insights on risk sources and their implications. The assessment phase follows, where identified risks are analyzed to determine their potential impact and likelihood. This phase employs statistical techniques and modeling tools to quantify the risks, allowing for a detailed evaluation of their significance.

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

In the mitigation phase, strategies and measures are developed to address the identified risks. This involves creating risk management plans that outline specific actions to reduce or eliminate the impact of risks. These strategies are informed by best practices in risk management and tailored to the unique challenges posed by Industry 4.0 technologies. The monitoring phase involves continuously tracking the effectiveness of the implemented risk management strategies and making adjustments as needed. This phase relies on real-time data collection and analysis facilitated by Industry 4.0 technologies, such as Cyber-Physical Systems (CPS), Internet of Things (IoT), and Cloud Computing, to ensure that the risk management processes remain effective and responsive to changing conditions. The methodology incorporates a cross-company orientation, extending traditional risk management approaches to consider interdependencies within the business ecosystem. This aspect of the methodology aims to identify and mitigate risks that arise not only within a single organization but also across its network of suppliers, customers, and competitors. The integration of cross-company perspectives is crucial for addressing the complexities introduced by digital advancements and ensuring a holistic approach to risk management in the context of Industry 4.0. This methodology provides a robust framework for understanding and managing risks in a rapidly evolving industrial environment, emphasizing the need for both internal and external considerations.

IV. RESULTS AND DISCUSSION

Table 1: Activities for implementing an integrated management system

Plan	Organisational vision and objectives	Establish policy (including ISMS policy), objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the organisation's overall policies and objectives.
Do	Processes	Implement and operate the policy, controls, processes and procedures.
Check	Performance	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act	Improvement	Take corrective and preventive actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement of the system.

The development of a suitable framework for integrating Enterprise Risk Management (ERM) and Information Security Management Systems (ISMS) into the Industry 4.0 concept represents a significant advancement for manufacturing companies. The proposed framework is designed to address the complex challenges associated with modern industrial environments, particularly those related to cybersecurity risks and the overall strategic risks of enterprises. The framework's design focuses on combining the key requirements of ERM and ISMS to create a comprehensive management system that supports the safe and efficient implementation of Industry 4.0 technologies.

The results from the integration of this framework demonstrate its effectiveness in minimizing enterprise risks by aligning the information security system with the broader corporate strategy. The structured approach outlined in Table 1, which encompasses the planning, implementation, performance assessment, and continual improvement phases, ensures that information security measures are consistently aligned with organizational objectives. This alignment is critical as it enables companies to manage and mitigate risks proactively while simultaneously enhancing their operational performance.

Furthermore, the integration of performance and risk management within this framework underscores the importance of embedding risk management practices into the core business processes. By adopting principles from Business Process Management (BPM) and Process Performance Management (PPM), the framework allows for the continuous

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

monitoring and assessment of process risks using real-time operational data, which is essential in the dynamic environment of Industry 4.0. The novel concept introduced in this framework also highlights the necessity of a governance structure that can effectively oversee business processes while ensuring that risks are managed in a way that supports the achievement of business goals.

The discussion also reveals that the implementation of this integrated management system leads to a more resilient and adaptable organizational structure. By defining clear data structures and indicators for risk assessment, the framework facilitates the identification and mitigation of risks before they can significantly impact business continuity or performance. Moreover, the ongoing assessment and regular updates of risk treatments and business continuity plans ensure that the framework remains relevant and effective in the face of evolving threats and challenges.

The framework developed in this study not only provides a robust method for managing risks in smart manufacturing environments but also offers a scalable solution that can be tailored to different organizational contexts. The integration of BPM, PPM, and risk management principles within this framework ensures that companies can achieve their strategic objectives while maintaining a high level of information security and operational efficiency. This integrated approach is crucial for the successful implementation of Industry 4.0 and the sustainable growth of manufacturing enterprises in the digital age.

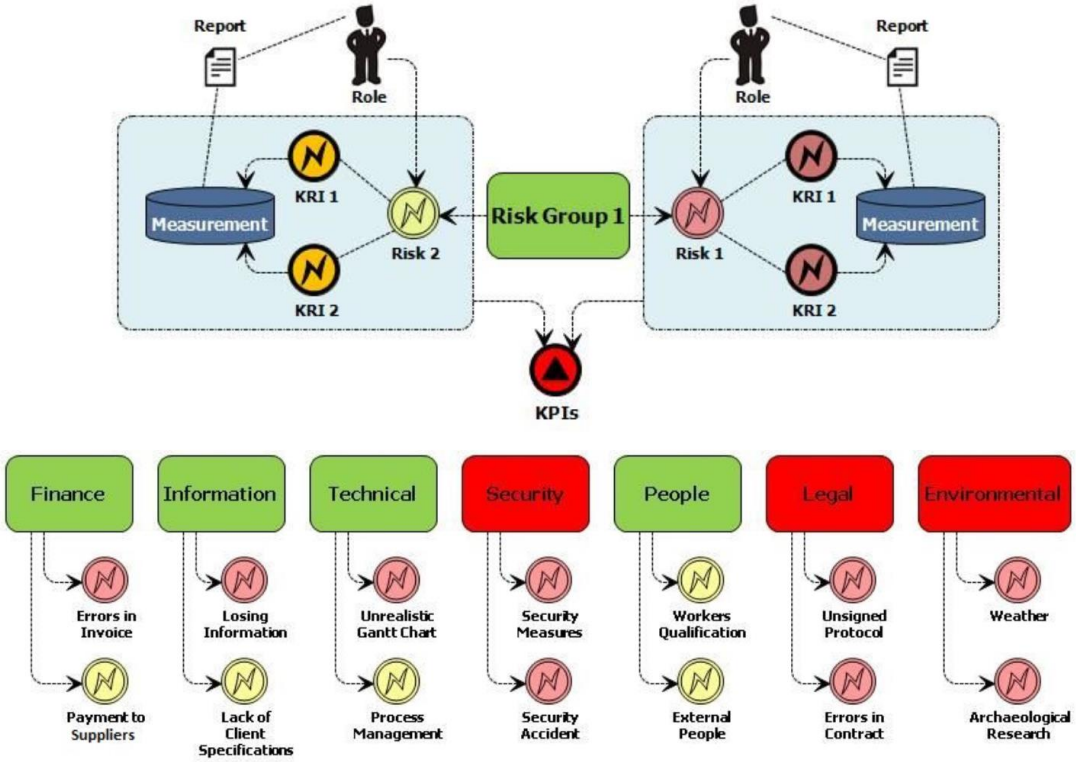

Figure 1: Model of risk groups and relationships between Risks - KRIs – KPIs

Given the extensive data generated from processes, it becomes possible to more accurately predict the types of potential damage and their likelihood of occurrence. However, this may require new assessment methods to handle the complexity of various scenarios effectively. Additionally, it may be necessary to adjust the criteria used for evaluating the probability of occurrence and the extent of potential damage.

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

To monitor risks effectively, Key Risk Indicators (KRIs) should be used to track how they influence Key Performance Indicators (KPIs) related to the organization's performance. This approach is illustrated in Figure 3. The identified risks are documented in a risk model, which categorizes them into significant groups to facilitate their management. Figure 3 uses different colors to distinguish between types of risks—such as operational risks (highlighted in red) and strategic risks (highlighted in yellow). These colors help in categorizing risks by their nature, priority, or assigned responsibilities. Furthermore, each major risk category can be subdivided into specific individual risks, as depicted in Figure 3, to provide a more detailed and structured risk assessment.

V. CONCLUSION

The primary objective of this paper was to explore and analyze the complexities of risk management within the context of Industry 4.0, with a focus on identifying and addressing the various aspects of risk management that are integral to its implementation. Through a comprehensive literature review, it became evident that the Industry 4.0 paradigm—characterized by the interconnectedness of humans, machines, and systems within dynamic, real-time, and self-organizing value creation networks—has a profound impact on all organizational processes. This interconnected environment necessitates the management of significantly larger volumes of data and demands real-time information handling capabilities, leading to the requirement for advanced infrastructures and adaptations in information management practices. The analysis revealed that the evolving conditions under Industry 4.0 are likely to introduce new types of risks, with a notable emphasis on information security challenges such as cyber-attacks and data integrity issues. These risks are anticipated to become more prevalent as the complexity and frequency of potential threats increase. Consequently, the nature of risk management processes will need to evolve to address these new vulnerabilities effectively. The study highlights that risk management strategies must adapt to the rapid advancements and challenges presented by Industry 4.0 to safeguard organizational operations and ensure the resilience of information systems in an increasingly digital and interconnected

REFERENCES

1. M. Hermann, T. Pentek, and B. Otto, Design Principles for Industrie 4.0 Scenarios: A Literature Review, 2015.
2. M. Lom, O. Pribyl, and M. Svitek, Industry 4.0 as a part of smart cities, in 2016 Smart Cities Symposium Prague (SCSP), 2016, pp. 1–6.
3. 2016 Global Industry 4.0 Survey. What we mean by Industry 4.0 / Survey key findings / Blueprint for digital success.
4. T. Niesen, C. Houy, P. Fettke, and P. Loos, Towards an Integrative Big Data Analysis Framework for Data-Driven Risk Management in Industry 4.0, in 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5065–5074.
5. M. Schröder, M. Indorf, and W. Kersten, Industry 4.0 and its impact on supply chain risk management, pp. 15–18, 2014.
6. M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective, World Acad. Sci. Eng. Technol. Int. J. Mech. Aerospace, Ind. Mechatron. Manuf. Eng. 8(1) (2014) 37–44.
7. S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, "Autonomous navigation robot", International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
8. S. Senthilkumar, C. Nivetha, G. Pavithra, G. Priyanka,S. Vigneshwari, L. Ramachandran, "Intelligent solar operated pesticide spray pump with cell charger", International Journal for Research & Development In Technology, vol. 7, no. 2, pp. 285-287, 2017.
9. D. Nathangashree, L. Ramachandran, S. Senthilkumar & R. Lakshmirekha, "PLC based smart monitoring system for photovoltaic panel using GSM technology", International Journal of Advanced Research in Electronics and Communication Engineering, vol. 5, no. 2, pp.251-255, 2016.
10. S. A. Malik and B. Holt, Factors that affect the adoption of Enterprise Risk Management (ERM)," OR Insight 26(4) (2013) 253–269.
11. KPMG, Enterprise Risk Management, An emerging model for building shareholder value, 2001.

ISSN(Online): 2320-9801

ISSN (Print): 2320-9798

International Journal of Innovative Research in Computerand Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 11, November 2019

12. Weber and R. Thomas, Key Performance Indicators: Measuring and Managing the Maintenance Function, 2005.
13. The Power of Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM).
14. S. Scandizzo, Risk Mapping and Key Risk Indicators in Operational Risk Management," Econ. Notes 34(2) (2005) 231–256
15. M. Stoll, From Information Security Management to Enterprise Risk Management, vol. 313. Cham: Springer International Publishing, 2015.