International Journal of Gender, Science and Technology
..ISSN: 2040-0748
UGC Care Group I Journal
Vol-12 Issue-01 May 2023

# DESIGN AND IMPLEMENTATION OF HYBRID APPROACH OF FIVE-DIMENSIONAL SUSTAINABILITY BASED ON SUPPLY CHAIN RISK MANAGEMENT SYSTEM IN TELECOMMUNICATION INDUSTRY

Dr.Y.Murali Mohan Babu
Professor, ECE Department
Chadalawada Ramanamma Engineering College, Tirupati, A.P, India
kisnamohanece@gmail.com

**ABSTRACT: In this paper design and implementation of hybrid approach of five dimensional sustainability based on supply chain risk management system in telecommunication industry is implemented. For term evaluation mainly every organization maintains the Sustainability for supply chain risk management. Basically, Supply chain manages the sustainability risks based on different methods.To get accurate & reliable results and manage the risks obtained, special technique is utilized. Hence in this supply chain sustainability risks management, a new three phase model is introduced. The main intent of this model is to identify and classify the risks obtained in supply chain. By using five dimensional approach the risk in the supply is categorized. Performance of this model is considered in the telecommunication industry. From results it can observe that hybrid approach of five dimensional sustainability based on supply chain risk management system gives effective outcome in terms of accuracy, security, cost and risks.**

***Keywords: Supply chain risk management, five dimensional sustainability approach, VLSI, Accuracy*.**

## I.INTRODUCTION

To improve the safety level in both industry and society, risk analysis plays major role. To develop the supply chain management, risk management and sustainability, different concepts are introduced based on the level of organization. But in supply chain management system risk plays major role [1]. Hence in this paper hybrid approach of five dimensional sustainability based on supply chain risk management system is introduced.

From figure (1) it can observe that the formation of sustainability based traditional supply chain risk management system. The supply chain risk management system performs the logistical operations. Therefore the supply chain risk management system is defined as the expansion of dimensions by integratingthe objectives of social and environmental [2]. In long term application supply chain management system plays very important role. It reduces the cost of system, increases the profit and allocates the resources to supply chain.


Fig. 1: Formation of sustainability based traditional supply chain risk management system

For organizations more risks are introduced and created based on the business practices of sustainability [3]. So the awareness of risk management should be done for the public of supply chain risks. Basically, depend on the complex and dynamic networks supply chain is defined. The supply chain management system solves the complex problems obtained while organizing the flow.

There are different methods in supply chain risk management system [5]. But mostly used method is FMEA. FMEA is nothing but failure mode and effects analysis. This concept is first introduced by the NASA program in 1960s. This method is considered as official method which evaluates the risk reliability by taking the requirements of safety [6]. FMEA identifies the risks of potential based on the single level and examine the effects in the system based on the higher levels. Therefore FMEA is widely used in the applications of electronics, nuclear, automotive, and aerospace to analyze the reliability of systems and safety [7-8].

Here the main thing is to use Cryptography is to secure the data. In electronic security systems these technology behave as a key role. To transfer money by using electronic, and IP secure and also automated signed files by using a techniques of Modern cryptography. Now a day's clients need to find the speed of the techniques in cryptographic because the usages of users are highly increases [9]. For example to identify physiology as well as surgery, it's a responsibility of doctor .Same as to secure the computer with cryptology with the help of security engineer. The main intention of this topic is without knowledge in cryptography. They don't know idea about before process.

To secure the data from unauthorized users and also to protect information from public access by using one of the security mechanisms is the Cryptography. By using cryptography to protect the data and resistant to attacks, it is a Greek origin word which means "secret writing" communicate between people in secretly by using a Classic cryptography. To change the message letters with other letters present this kind of cryptography is commonly applied. Nowadays based on demand by the users to change into algorithm based cryptography. Here to perform operation in 2 processes that is encryption and decryption, to convert the original data to encrypt data using a particular algorithm is possible only to perform encryption process. Here to perform decryption process to change the original data into encrypted data because the process of decryption is opposite process of encryption

Cryptography is the process of hiding confidential information from third parties through the use of keys known only to the communicating parties. It is a secure form of communication, so that bank card payments and electronic building can be used for electronic commerce. With proper implementation, cryptography can help to secure online servers. Improper cryptographic applications reveal sensitive information and provide the user with a false sense of security.

Encryption is essential for protecting sensitive data from eavesdroppers, attackers, and unauthorized users. Such protocols have a wide range of applications, from Internet banking to the Internet of things. As the Internet of Things (IOT) becomes more popular, it is essential to ensure that connected devices are authenticated. When an unknown user attempted to disrupt communication between two authorized devices, we were subjected to a slew of attacks [10]. The devices are typically linked using a handshake protocol in which they agree on a simple encryption algorithm to use, establishing a secure communication medium and sharing the necessary key

## II. VLSI SUPPLY CHAIN SECURITY RISKS

The present semiconductor industry includes various business substances on a worldwide scale in plan, fabricating, framework joining and circulation of VLSI chips and frameworks. Without a successful security component, a rebel component in this interaction -, for example, an IP supplier, an IC plan house, a CAD organization, a foundry, a wholesaler or a framework integrator - can undoubtedly take plan IPs or alter an IC plan; there is likewise a likelihood that an outcast enemy takes plan IPs or alters the plan.

### 2.1. IP THEFT AND MISUSE

IC plans and the intellectually properties (IPs) made during the plan cycle can be safeguarded lawfully through the means like patent, copyright, brand name, and proprietary advantage. Plan IPs, (for example, Verilog code, plan information, and FPGA setup bit-stream records) can likewise be encoded to forestall unlawful duplicate or abuse. Notwithstanding, IP burglary is a simple and truly beneficial business practice because of the absence of successful regulation requirement components, and the need of keeping IP simple to utilize and reuse. Clearly, we have seen wild IP burglary and abuse in semiconductor industry as of late.

For instance, in over-building, an agreement maker takes care of a request and keeps on building more chips and sells them. In cloning, a contender makes a duplicate of a plan by taking part or the entirety of a framework's protected innovation (IP). In picking apart, a contender separates every one of the IPs from a plan, yet in addition express subtleties on how the plan functions - by bundle expulsion, delayering, imaging, circuit extraction and investigation - which permits the IPs to be reused, improved, or camouflaged to foil conceivable lawful activity

### 2.2. IC TAMPER

The finished results of IP burglary and abuse are frequently known as fakes, which are work-the same or cloned items with illicit utilization of a brand name. Such fakes are inescapable; the United States

Department of Defense has distinguished more than 1,000,000 speculate fake parts related with production network splits the difference in two years. Such fake chips might be produced using reused chips of debased lifetime, dependability or execution.

The most extreme type of equipment security chances is that on such fake chips an enemy might mess with the veritable plan and introduce a "Deception" part which once set off goes about as a rationale bomb or data spill indirect access. A whole Trojan program might be concealed in equipment, e.g., in a Trojan ROM next to a processor. An enemy might send off such an assault from a foundry, from a framework sequential construction system, or anybody who catches an equipment gadget might supplant an authentic chip with a fake chip on a printed-circuit board (PCB).

An altered framework might in any case work true to form for least impression, then again, actually it gives a secret assault instrument to learned aggressors. Such IC alter assaults might sidestep all the current security arrangements carried out at higher (e.g., programming application or working framework) levels. For instance, the current static and dynamic code uprightness confirmation strategies recognize alter in the record framework, memory or stack rather than an equipment Trojan.

Thus, IC alter assaults compromise a key presumption of the current security framework plans which is the dependability of equipment. They demand genuine reevaluating on security framework plan. IC alter assaults may not prompt clear benefit, while stowed away motivations can't be precluded, since potential aggressors, for example, beginner programmers, criminal associations and country states have various assets, limits and impetuses.

Now and again, IC alter can be a monetarily suitable practice, for instance, introducing information gathering equipment spyware. Because of the expected seriousness of such assaults and the impediments of the current countermeasure methods, the Comprehensive National Cyber Security Initiative has recognized this production network hazard the executives issue as a top public need

## III. HYBRID APPROACH OF FIVE-DIMENSIONAL SUSTAINABILITY BASED ON SUPPLY CHAIN RISK MANAGEMENT SYSTEM

The below figure (2) shows the flow chart of hybrid approach of five dimensional sustainability based on supply chain risk management system. The entire method is divided into two phases. Phase-1 is performed when risk is found and phase-2 is performed when risk is not found. In this initially the input data is configured using data confirmation block. Next sample data is selected. Now, from this sample data risk is identified. If the risk found critical then phase-1 operation is performed. If the risk doesn't found critical then phase-2 operation is performed.

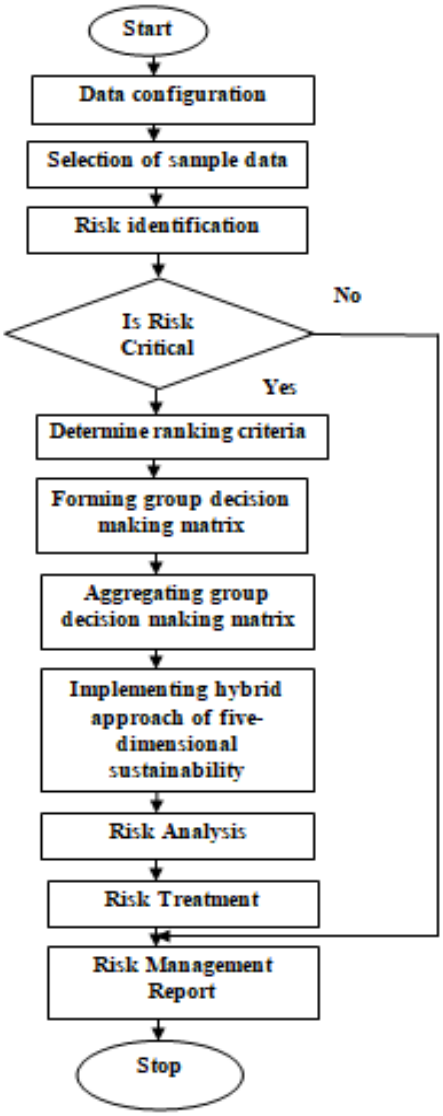


Fig. 2: Flow chart of hybrid approach of five dimensional sustainability based on supply chain risk management system

In phase-1, risk is critical. After risk is identified then ranking criteria is determined. Next group decision

making matrix is formed. After formation of group decision making matrix, aggregation of group decision making matrix is performed. Now, hybrid model is applied to the obtained data. After this analysis of risk is performed. Then treatment of risk is performed for the obtained data. At last risk management report is obtained.

In phase-2, risk is not critical. Then directly the risk management report is obtained.

Algorithm:

Step-1: The entire method is divided into two phases.

Step-2: Phase-1 is performed when risk is found and phase-2 is performed when risk is not found.

Step-3: In this initially the input data is configured using data confirmation block.

Step-4: Next sample data is selected.

Step-5: Now, from this sample data risk is identified. If the risk found critical then phase-1 operation is performed.

Step-6: If the risk doesn't found critical then phase-2 operation is performed.

Step-7: In phase-1, risk is critical.

Step-8: After risk is identified then ranking criteria is determined.

Step-9: Next group decision making matrix is formed.

Step-10: After formation of group decision making matrix, aggregation of group decision making matrix is performed.
Step-11: Now, hybrid model is applied to the obtained data.

Step-12: After this analysis of risk is performed.

Step-13: Then treatment of risk is performed for the obtained data.

Step-14: At last risk management report is obtained.

Step-15: In phase-2, risk is not critical.

Step-16: Then directly the risk management report is obtained.

The below table (1) shows the comparison table of supply chain risk management system and hybrid approach of five dimensional sustainability based on supply chain risk management system. In this accuracy, cost, number of risks, time and security parameters are there. Compared with supply chain risk management system, hybrid approach of five dimensional sustainability based on supply chain risk management system will improves the accuracy and security and reduces the cost, number of risks and time.

TABLE. 1: COMPARISON TABLE

| S.NO | Parameters | Supply Chain Risk Management System | Hybrid Approach Of Five Dimensional Sustainability Based On Supply Chain Risk Management System |
|---|---|---|---|
| 1 | Accuracy | 53% | 94% |
| 2 | Cost | 86% | 12% |
| 3 | Number of risks | 96% | 7% |
| 4 | Time | 84% | 10% |
| 5 | Security | 11% | 96% |

The below figure (3) shows the comparison of accuracy and time for supply chain risk management system and hybrid approach of five dimensional sustainability based on supply chain risk management system. Compared with supply chain risk management system, hybrid approach of five dimensional sustainability based on supply chain risk management system will improves the accuracy and reduces the time.

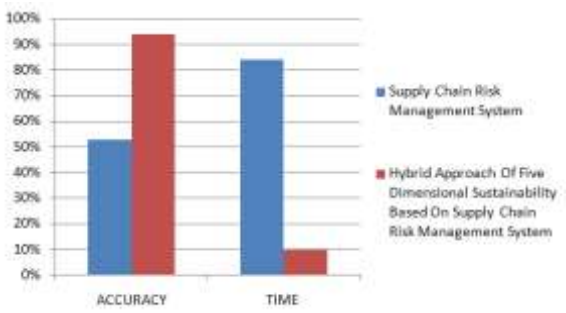

Fig. 3: Comparison of accuracy and time

The below figure (4) shows the comparison of cost and number of risks for supply chain risk management system and hybrid approach of five dimensional sustainability based on supply chain risk management system. Compared with supply chain risk management system, hybrid approach of five dimensional sustainability based on supply chain risk management system will reduces the cost and risks.


Fig. 4: Comparison of cost and number of risks

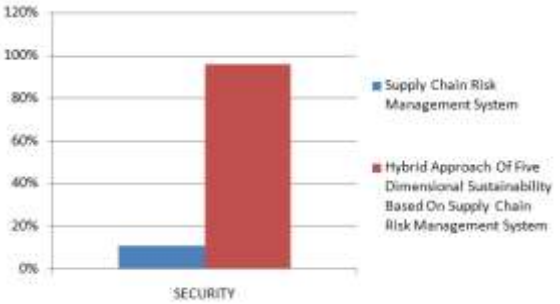


Fig. 5: Comparison of security

## IV. CONCLUSION

Hence in this paper design and implementation of hybrid approach of five dimensional sustainability based on supply chain risk management system in telecommunication industry was implemented. The entire method is divided into two phases. Phase-1 is performed when risk is found and phase-2 is performed when risk is not found. In this initially the input data is configured using data confirmation block. Next sample data is selected. Now, from this sample data risk is identified.From results it can observe that hybrid approach of five dimensional sustainability based on supply chain risk management system gives effective outcome in terms of accuracy, security, cost and risks.

## V. REFERENCES

[1]. Goodarzian. F., Hosseini-Nasab. H., Fakhrzad. M. B., A Multiobjective Sustainable Medicine Supply Chain Network Design using a Novel Hybrid Multi-Objective Metaheuristic Algorithm, International Journal of Engineering, Transactions A: Basics Vol. 33, No. 10, (2020) 1986-1995, doi: 10.5829/IJE.2020.33.10A.17.

[2]. Ebinger. F. Omondi. B., Leveraging Digital Approaches for Transparency in Sustainable Supply Chains: A Conceptual Paper, Sustainability, Vol. 12, No. 12, (2020) 6129, doi" 10.3390/su12156129.

[3] Nimsai. S., Yoopetch. C., Lai, P., Mapping the Knowledge Base of Sustainable Supply Chain Management: A Bibliometric Literature Review, Sustainability, Vol. 12, No. 18, (2020) 7348, doi: 10.3390/su12187348.

[4]. Akbari-Kasgari. M., Khademi-Zare. H., Fakhrzad. M.B., M. Hajiaghaei-Keshteli. M., Honarvar. M., A Closed-loop Supply Chain Network Design Problem in Copper Industry, International Journal of Engineering, Transactions A: Basics Vol. 33, No. 10, (2020) 2008-2015, doi: 10.5829/IJE.2020.33.10A.19.

[5]. Rezaei. S., Maihami. R, Optimizing the sustainable decisions in a multi-echelon closed-loop supply chain of the manufacturing/remanufacturing products with a competitive environment. Environment, Development and Sustainability, Vol. 22, No 1, (2019) 1-27, doi: 10.1007/s10668-019-00491-5.

[6]. Kaur. A., Sharma. P. C., Social sustainability in supply chain decisions: Indian manufacturers. Environment, development and Sustainability, Vol. 20, No. 4, (2018) 1707-1721, doi: 10.1007/s10668-017-9961-5.

[7]. Giannakis. M., Papadopoulos. T., Supply chain sustainability: A risk management approach, International Journal of Production Economics, Vol. 171, No. 4, (2016) 455-470, doi: 10.1016/j.ijpe.2015.06.032.

[8] Vahdani. B., Salimi. M., Charkhchian. M., A new FMEA method by integrating fuzzy belief structure and TOPSIS to improve risk evaluation process, The International Journal of Advanced Manufacturing Technology, Vol. 77, No. 1, (2015) 357-368, doi: 10.1007/s00170-014-6466-3.

[9] Liu. H. C., You. J. X., You. X. Y., Shan. M. M., A novel approach for failure mode and effects analysis using combination weighting and fuzzy VIKOR method, Applied Soft Computing, Vol. 28, No. C, (2015) 579-588, doi: 10.1016/j.asoc.2014.11.036.

[10] 27. Lolli. F., Ishizaka. A., Gamberini. R., Rimini. B., Messori. M., FlowSort-GDSS–A novel group multi-criteria decision support system for sorting problems with application to FMEA, Expert Systems with Applications, Vol. 42, No. 17, (2015) 6342-6349, doi: 10.1016/j.eswa.2015.04.028.

[11] 28. Song. W., Ming. X., Wu. Z., Zhu. B., A rough TOPSIS approach for failure mode and effects analysis in uncertain environments, Quality and Reliability Engineering International, Vol. 30, No. 4, (2014) 473-486, doi: doi.org/10.1002/qre.1500.

[12] Hadi-Vencheh. A., Aghajan. M., Failure mode and effects analysis: A fuzzy group MCDM approach, Journal of Soft Computing and Applications, Vol. 1, No. 14, (2013), doi: 10.5899/2013/jsca-00016

[13] Chang. K. H., Cheng. C. H., A risk assessment methodology using intuitionistic fuzzy set in FMEA, International Journal of Systems Science, Vol. 41, No. 12, (2010) 1457-1471, doi: 10.1080/00207720903353633.

[14] Chin. K. S., Wang. Y. M., Poon. G. K. K., Yang. J. B., Failure mode and effects analysis by data envelopment analysis, Decision Support Systems, Vol. 48, No. 1, (2009) 246-256, doi: 10.1016/j.dss.2009.08.005.

[15] Stock. J. R., Boyer. S. L., Developing a consensus definition of supply chain management: a qualitative study. International Journal of Physical Distribution and Logistics Management, Vol. 39, No. 8, (2009) 690-711, doi: 10.1108/09600030910996323.