2019 Proceedings of PICMET '19: Technology Management in the World of Intelligent Systems

# An Intelligent Risk Management Model for Achieving Smart Manufacturing on Internet of Things

Joseph S.M. Yuen, K.L. Choy, H.Y. Lam, Y.P. Tsang
Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong

***Abstract*—To adapt to the ever-changing environment, Internet of Things (IoT) has emerged for supporting manufacturing plants to better manage the quality of products. Since the application of IoT is relatively new to the manufacturing industry, increasing attention has been paid on how to manage the planning and implementation process so as to achieve smart manufacturing. However, IoT applications in each manufacturing plant are varied due to different specifications, such as the product types, product nature, plant layout, production flow, machine and equipment settings. Hence, it is essential to perform risk analysis to ensure that any possible situation and uncertainty is being considered before the implementation process. Risk management plays an important role since disruption can cause significant financial and reputational loss, especially for electronics products, which are environmental-sensitive. In this study, an electronic manufacturing risk management model (EM-RMM) is designed to assess the risk faced by manufacturing plants for IoT applications. By identifying the risks faced by manufacturing plants for IoT applications, the likelihood and consequences of the risks are analyzed by using fuzzy analytical hierarchy process (FAHP) to calculate the weighting of the risks. Through a case study in a plant which manufactures environmental-sensitive electronics products, the results provide a systematic procedure for risk assessment in IoT implementation, with the aim of achieving smart manufacturing.**

## I. INTRODUCTION

As the demand for high-tech products increases, it requires enhancements in quality and function, particularly for electronic products. To adapt to the ever-changing environment in the manufacturing industry, the concept of smart manufacturing has emerged to improve productivity and accelerate innovation [1][2]. With the support of information technologies, a manufacturing firm can better manage the quality of a product. To achieve smart manufacturing, Internet of Things (IoT) is considered as an emerging technology in the manufacturing process. According to Gubbi et al. [3], IoT is the interconnection of sensing devices which provide the ability to share information across different platforms through a unified framework developing a common operating platform to enable innovative applications. Although IoT is becoming popular in the manufacturing industry, IoT applications in each manufacturing plant are varied due to different specifications of manufacturing plants [4]. Due to a lack of knowledge and experience in IoT implementation, the manufacturing company is often unable to implement IoT technology in the existing workflow for effectively enhancing the quality of electronic products. In addition, during the IoT implementation process, it is expected that different risks may be encountered which may lead to project failure. For example, electronic products are environmentally sensitive and need to be manufactured under certain temperature and humidity condition. It becomes essential to keep monitoring the working environment in real time and ensure that the data can be collected and stored accurately during IoT implementation. Therefore, an appropriate risk management approach becomes important in IoT implementation for electronics products manufacturing.

In this paper, an electronic manufacturing risk management model (EM-RMM) is designed to assess the risk faced by manufacturing plants for IoT applications. By applying a fuzzy analytical hierarchy process (FAHP), which is a multiple criteria decision-making technique, the potential risk factors that may occur in IoT implementation are identified and analyzed based on their likelihood of occurrence and their consequences. As a result, the potential risk that has highest weighting is considered as the most important risk that requires additional attention in order to mitigate its impact. This study shows a high relevance to technology management in terms of system planning and implementation. According to Kearns et al. [5], technology management is of strategic importance to the organizations by combining engineering and management knowledge in problem solving of technology-related projects. Through the design and planning process, it suggests how the IoT technology can be implemented in the manufacturing plants which handle environmental sensitive products. Any possible risk that may incur during implementation is considered in order to ensure that the new IoT technology project can be executed smoothly. To summarize, the study contributes to a practical approach in managing IoT technology implementation so as to increase the competiveness in the manufacturing industry. This paper is organized as follows. Section 2 covers the past literature related to IoT for smart manufacturing, risk management in IoT applications, and the fuzzy analytical hierarchy process (FAHP) for risk management. Section 3 presents the design of the electronic manufacturing risk management model (EM-RMM). Section 4 presents a case study in an electronics manufacturing plant, while the results and discussion are presented in Section 5. Finally, the conclusions are drawn in Section 6.

## II. LITERATURE REVIEW

### *A. IoT for Smart Manufacturing*

As the manufacturing process has become automated, computerized and complex, the future development in the manufacturing industry becomes technology-oriented. Sensors and data intensive modelling that arise from the concept of the cyber-physical system, such as IoT and cloud computing, are the

978-1-890843-39-7 © 2019 PICMET

trends for achieving smart manufacturing. Internet of Things (IoT) is the network that connects internet-enabled objects with the web/intenet service without human handling, and was introduced as early as 1980's. With the mature development in technology, the application of IoT has gained increasing attention to connect, interact and exchange data [6][7]. The IoT solution requires an integration of software and hardware components for the multi-layers of technologies. A typical IoT technology stack is composed of the three main layers, the thing or device layer, the connectivity layer and the IoT cloud layer. At the thing or device layer, the new hardware such as sensors and processors are added to the existing hardware. The additional hardware can help to monitor, manage and operate the physical things. At the connectivity layer, the communication protocols can enable the communication between the individual physical hardware and the cloud. At the IoT cloud layer, software is used for communication, for example, for storing data and assessing the data [8]. Shrouf and Miragliotta [9] applied IoT in production management. Wang and Wang [10] designed a cloud-based production system for handling waste electronics by IoT. Tao et al. [11] used IoT for achieving smart manufacturing based on a cyber-physical system. The above studies showed that the adoption of IoT can enhance the operational efficiency in the manufacturing industry.

### B. *Risk Management in IoT Applications*

Risk is defined as the probability of occurrence of an event within a specific period of time, in which we have to eliminate or mitigate the negative consequences of such a risk [12]. Risk management is always a difficult task because it is difficult to estimate the probability of certain events occurring [13]. A disruption at any stage in the supply chain can lead to large financial and reputational losses which is the reason for the existence of supply chain risk management. In the literature, it is found that attention was mainly focused on risk management in various kinds of projects, such as construction projects [14][15], new project development projects [16][17], and, software and IT projects [18][19][20]. However, in the context of IoT implementation, only limited research has been conducted to investigate the success factors for an IoT project. Akhtar et al. [21] considered information processing capabilities and operational agility were the important success factors of an IoT project. Kim et al. [22] mentioned that information quality was the primary concern when designing an IoT solution for a real time scheduling problem. Although IoT has drawn significant research attention due to its ability to increase information visibility, there is lack of a comprehensive approach to manage the potential risks that may occur in the IoT implementation process.

### C. *Fuzzy Analytical Hierarchy Process (FAHP) for Risk Management*

Multiple criteria decision-making (MCDM) techniques such as the analytical hierarchy process (AHP) and fuzzy analytical hierarchy process (FAHP) are commonly used in risk management [23]. Unlike the general risk filtering and ranking management (RFRM) approach that only weigh the risk factors based on likelihood and consequence, AHP is a systematic decision-making tool to solve MCDM problems [24]. It decomposes a complex MCDM problem into a system of hierarchies by standardizing the numeric scale for the measurement of quantitative as well as qualitative performance. Although AHP has been widely adopted to solve the multi-criterion decision making problems, its most important drawback is that the use of a scale of 1 to 9 cannot handle the uncertainty decisions when making comparison of the attributes. It may not be accurate for the decision makers to assign a discrete value of the pairwise judgement. The decision maker needs other measures to describe the vagueness rather than the distinct nine-point scale. By integrating fuzzy logic approach to the AHP process, triangular fuzzy numbers (TFNs) are therefore used to decide on the priority of one decision over another. Wang et al. [25] attempted to use the FAHP method to have a structured analysis of the aggregative risk of implementing green initiatives in the fashion industry supply chain for risk assessment. Khodadadi & Kumar [26] applied the FAHP method to identify all the risks involved for selecting a contractor, in which the weakness of each contractor can be figured out and used for decision making.

In summary, it is found that the smart manufacturing and IoT applications are the major trends in the future manufacturing industry. It is essential to implementing the IoT technology in the existing workflow to facilitate the manufacturing process. Moreover, it is important for the manufacturing companies to manage the risk, since risk can lead to the failure of manufacturing companies. When assessing risk in IoT application, since the type of potential risks may not be able to compare using distinct numbers only, fuzzy logic is combined with AHP to design the proposed EM-RMM model which allows the decision maker to give a comparative response between two criteria.

## III. Design of Electronic Manufacturing Manufacturing Risk Management Model

The system architecture of the electronic manufacturing risk management model (EM-RMM) is shown in Fig. 1. It consists of three major tiers: data collection, FAHP model and strategy formulation.

### A. *Tier 1: Data Collection*

Tier 1 includes the redesign of the workflow for including the IoT implementation and the risk data collection for implementing the new workflow. The workflow is redesigned to include the IoT implementation. It is important to monitor the temperature and humidity of the environment for the whole electronic manufacturing process. As a result, temperature and humidity sensors are added, and the real-time data are transmitted to the centralized cloud database. Through the redesigned workflow, some useful data can be obtained from the IoT implementation. For example, environmental information, including temperature and humidity, product information including the location and quantity, and risk data information including the likelihood and consequence. These useful data are transmitted wirelessly and stored in the centralized cloud database. The centralized cloud database can be accessed via the devices that are connected to the system.

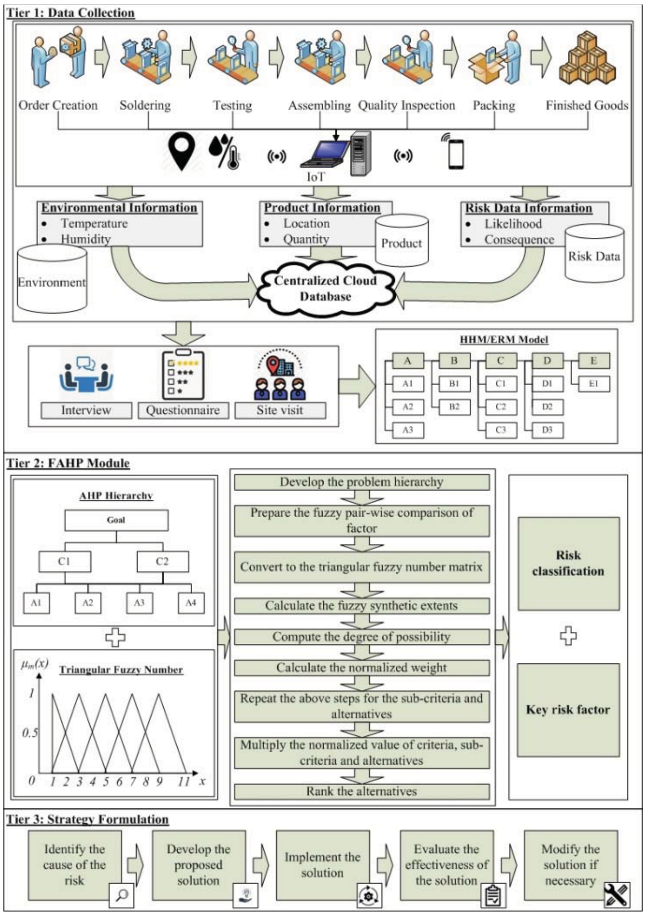


Fig. 1. Design of the electronic manufacturing risk management model

After the workflow is redesigned, the risk data for implementing the new workflow is collected by questionnaire, site visits and interviewing the management and the workers for opinions. Through interviews and site visits, the potential risk factors can be identified and classified. All the potential risk factors can be listed that considers the decomposition of the main risk factors. In the meantime, the score of likelihood and the consequences of these potential risks are recorded by questionnaire. Then, all the risk data are ready for the FAHP module for the risk assessment.

## B. Tier 2: FAHP Module

In Tier 2, the FAHP module is used for finding the key risk factor. Firstly, the problem hierarchy is developed. The hierarchy levels from top to bottom are goal, criteria, sub-criteria, and alternatives respectively. Then, fuzzy pair-wise comparison of the factors is conducted for identifying the intensity of importance of one criterion over another criteria. Table I shows the FAHP pairwise comparison scale from $M_1$ to $M_5$. The higher the scale, the higher the importance over another criterion. The fuzzy pair-wise comparison result is then converted into a triangular fuzzy number matrix. The triangular fuzzy number is ($l$, $m$, $u$), which represent the lower, mean and upper values respectively. The triangular fuzzy reciprocal number is ($1/u$, $1/m$, $1/l$). The fuzzy synthetic extent value ($D_i$) with respect to the $i^{th}$ criterion is then calculated using (1).

TABLE I. FAHP PAIRWISE COMPARISON SCALE

| Intensity of Importance | Fuzzy number | Triangular fuzzy numbers |
|---|---|---|
| Equally important | M1 | (1, 1, 1) |
| Moderately more important | M2 | (1, 2, 3) |
| Strongly more important | M3 | (2, 3, 4) |
| Strongly important | M4 | (3, 4, 5) |
| Extremely important | M5 | (4, 5, 6) |

$$D_i = \sum_{j=1}^{n} \alpha_{ij} \otimes \left[\sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij}\right]^{-1} \tag{1}$$

The degree of possibility between two triangular fuzzy numbers $M_1(l_1, m_1, u_1)$ and $M_2(l_2, m_2, u_2)$ can be calculated using (2). By selecting the minimum value, the degree of possibility of criteria $Ci$, can be obtained by (3)

$$P(M_1 \geq M_2) = \begin{cases} 1 & m_1 \geq m_2 \\ \frac{l_2 - u_1}{(m_1 - u_1)(m_2 - l_2)} & m_1 \leq m_2, u_1 \geq l_2 \\ 0 & otherwise \end{cases} \tag{2}$$

$$d(C_i) = min\, P\left(M_{C_i} \geq M_{C_j}\right) \qquad \forall i, i \neq j \tag{3}$$

Subsequently, the normalized weights of each criteria are calculated by (4). The steps are then repeated to calculate the weight ($Ws_i$) of the sub-criteria ($S_i$) and the value ($V_{Ai}$) of the alternatives ($A_i$). By calculating the total weight of the sub-criteria $S_i$ ($TW_{Si}$) and the total value of the alternatives $A_i$ in the sub-criteria $S_i$ ($TV_{SiAi}$) using (5) and (6) respectively, the total value of the alternatives $A_i$ can be obtained. By using the result of the total value of the alternative, the priority in choosing the alternatives can be ranked in descending order.

$$W_{C_i} = d(C_i) \times \left(\sum_{i=1}^{n} d(C_i)\right)^{-1} \tag{4}$$

$$TW_{S_i} = W_{C_i} \times W_{S_i} \tag{5}$$

$$TV_{S_i A_i} = V_{A_i} \times TW_{S_i} \tag{6}$$

## C. Tier 3:Strategy Formulation

Tier 3 is used for strategy formulation for solving the potential risk factors. To identify the root cause of the risk, it is needed to determine which part of the manufacturing process has gone wrong and lead to the potential risk happening. Also, it is important to understand the nature of the risk to obtain a solution. After understanding the nature of the risk in term of likelihood and consequence, the risk can be classified.

For a risk with a low level of consequence and low level of likelihood, the proposed solution should be considered as accepting the risk. For the risk with a low level of consequence and high level of likelihood, the proposed solution should be considered as avoiding the risk. For the risk with a high level of consequence and low level of likelihood, the proposed solution should be considered as transferring the risk. For the risk with the nature of high level of consequence and high level of likelihood, the proposed solution should be considered as mitigating the risk.

Then, an action plan is required to show how to implement the solution. After the action plan is developed and implemented, it is important to evaluate the effectiveness of the solution and how it can reduce or eliminate the risk. Finally, if it is found that the effectiveness of implementing the solution is low, it means that the solution cannot effectively aim at reducing the level of consequence and likelihood of the risk. Therefore, it is necessary to modify the solution for improvement.

## IV. CASE STUDY

Innovation Sound Technology Co. Ltd. is a manufacturing company located in Shenzhen China. It mainly produces high quality audio equipment such as headsets, headphones, and earphones. The company has more than ten working stations and storage areas with different requirements on ambient temperature and relative humidity. In order to increase the information visibility along the production lines, the company decided to implement IoT solutions in their daily production processes. In addition to the layout setting and workflow redesign to suit the needs of IoT adoption, the company also considers the need for risk management that may be required during the implementation process. Therefore, the EM-RMM is designed and applied in the company as a pilot study. The implementation of EM-RMM is divided into two phases, i.e. key risk factors identification and pair-wise comparison.

### A. *Key Risk Factors Identification*

In this phase, the key risk factors are identified for implementing IoT in the electronics manufacturing process. By conducting interviews with the managerial staff in the case company, the potential risk factors are identified. Fig. 2 shows the 3-level hierarchy for key risk factor identification. With the goal of identifying the key risk factors for implementing IoT in electronics manufacturing process, two criteria are identified. They are likelihood (C1) and consequence (C2). Likelihood (C1) refers to the frequency that the risk will happen, and measures how often will the risk scenario occur when implementing IoT in the electronics manufacturing process. Consequence (C2) refers to the damage or losses resulting from the risk scenario occurring. It measures how the severity of the risk affects the electronics manufacturing operation. Two sub-criteria of each criteria are then identified. For the Likelihood (C1), the sub-criteria include suddenly (C11) and occasionally (C12), which show the frequency of occurrence. Suddenly (C11) refers to any unexpected event that may occur without warning, while occasionally (C12) refers to an event that may occur periodically or happen more than once. For the Consequence (C2), two measures, i.e. monetary value (C21) and time (C22), are identified as the sub-criteria. Monetary value (C21) considers the financial loss if the risk occurs, while time (C22) considers whether a large amount of time is required to tackle the risk. The last level in the hierarchy is the decision alternatives, and they refer to the potential risks in IoT implementation. The potential risks are classified into three categories, i.e. operations (R1), labor (R2), and, system and information (R3).

Operations (R1) refers to the factors that affect the working of the manufacturing process, and consists of five potential risks: breakdown of the facilities (R11), workflow redesign (R12), unstable wireless internet network (R13), improper operation (R14) and power failure (R15). Since electronics manufacturing requires many different machines for the operation, any breakdown of the facilities (R11) will decrease productivity. For workflow redesign (R12), there may be some changes in the operations process when implementing IoT. Therefore, the risk of workflow redesign may occur during the implementation process which may affect the productivity. An unstable wireless internet network (R13) would affected the daily operations in data capturing. Since the use of IoT relies on a stable network in order to transfer the data to the database, a stable wireless internet connection is an important concern. Improper operation (R14) refers to the misuse of the sensing and data capturing equipment. Since the implementation of IoT requires a setup of sensors and data capturing equipment, an interruption of the manufacturing process may occur if there is improper use of equipment in the manufacturing operations. Power failures (R15) refers to the shortages of the electricity supply which cannot provide enough power to support the equipment operations.

Labor (R2) refers to the factors related to human resources. The sub-criteria includes resistance to change (R21) and lack of knowledge in IoT adoption (R22). For resistance to change (R21), since the adoption of IoT would result in changes to the existing manufacturing process, and workers who are familiar with the current operations may not be willing to make any change easily. For the lack of knowledge in IoT adoption (R22), it is found that most of the workers have a low-level education background. They may not have the skills to use the IoT equipment properly, thus affecting the operations performance.

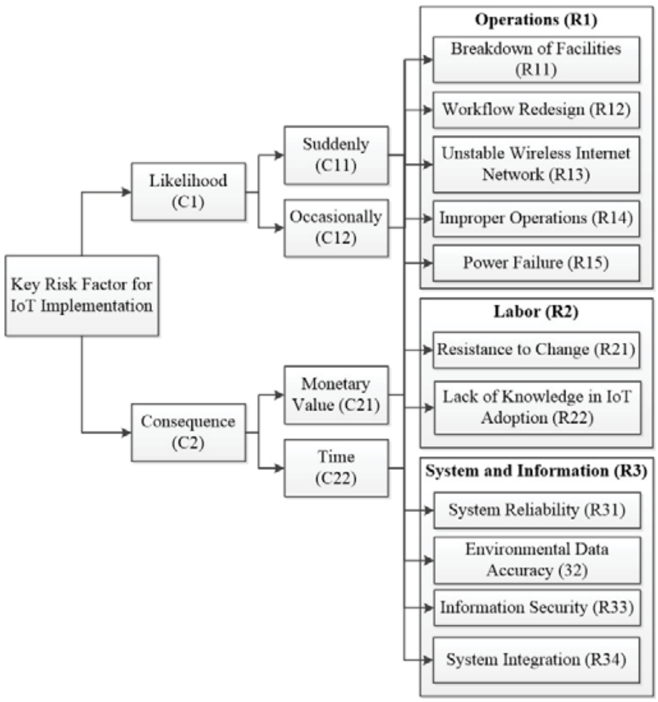


Fig. 2. 3-level hierarchy for key risk factor identification

TABLE II. FUZZY COMPARISON MATRIX FOR ALTERNATIVES TO THE SUB-CRITERIA (MONETARY VALUE) WITH DEGREE OF FUZZINESS = 1

| | R11 | | | R12 | | | R13 | | | R14 | | | R15 | | | R21 | | | R22 | | | R31 | | | R32 | | | R33 | | | R34 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R11 | 1 | 1 | 1 | 4 | 5 | 6 | 2 | 3 | 4 | 2 | 3 | 4 | 1.0 | 2 | 3 | 0.25 | 0.33 | 0.5 | 0.25 | 0.33 | 0.5 | 0.33 | 0.5 | 1 | 0.2 | 0.25 | 0.33 | 1 | 1 | 1 | 1 | 2 | 3 |
| R12 | 0.17 | 0.2 | 0.25 | 1 | 1 | 1 | 0.2 | 0.25 | 0.33 | 0.17 | 0.2 | 0.25 | 0.25 | 0.33 | 0.5 | 0.33 | 0.5 | 1 | 0.33 | 0.5 | 1 | 0.25 | 0.33 | 0.5 | 0.17 | 0.2 | 0.25 | 1 | 1 | 1 | 0.33 | 0.5 | 1 |
| R13 | 0.25 | 0.33 | 0.5 | 3 | 4 | 5 | 1 | 1 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 1 | 2 | 3 | 1 | 2 | 3 | 0.25 | 0.33 | 0.5 | 1 | 2 | 3 | 2 | 3 | 4 |
| R14 | 0.25 | 0.33 | 0.25 | 4 | 5 | 6 | 0.25 | 0.33 | 0.5 | 1 | 1 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 3 | 4 | 5 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 2 | 3 | 4 | 2 | 3 | 4 |
| R15 | 0.33 | 0.5 | 1 | 2 | 3 | 4 | 0.33 | 0.5 | 1 | 0.25 | 0.33 | 0.5 | 1 | 1 | 1 | 1 | 2 | 3 | 2 | 3 | 4 | 2 | 3 | 4 | 1 | 2 | 3 | 1 | 2 | 3 | 2 | 3 | 4 |
| R21 | 2 | 3 | 4 | 1 | 2 | 3 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 0.33 | 0.5 | 1 | 1 | 1 | 1 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 1 | 1 | 0.2 | 0.25 | 0.33 | 0.33 | 0.5 | 1 |
| R22 | 2 | 3 | 4 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 0.2 | 0.25 | 0.33 | 0.25 | 0.33 | 0.5 | 0.33 | 0.5 | 1 | 1 | 1 | 1 | 0.25 | 0.33 | 0.5 | 0.17 | 0.2 | 0.25 | 0.33 | 0.5 | 1 | 0.33 | 0.5 | 1 |
| R31 | 1 | 2 | 3 | 2 | 3 | 4 | 0.33 | 0.5 | 1 | 0.33 | 0.5 | 1 | 0.25 | 0.33 | 0.5 | 0.33 | 0.5 | 1 | 2 | 3 | 4 | 1 | 1 | 1 | 0.33 | 0.5 | 1 | 2 | 3 | 4 | 1 | 2 | 3 |
| R32 | 3 | 4 | 5 | 4 | 5 | 6 | 2 | 3 | 4 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 1 | 1 | 1 | 4 | 5 | 6 | 1 | 2 | 3 | 1 | 1 | 1 | 2 | 3 | 4 | 3 | 4 | 5 |
| R33 | 1 | 1 | 1 | 1 | 1 | 1 | 0.33 | 0.5 | 1 | 0.25 | 0.33 | 0.5 | 0.33 | 0.5 | 1 | 3 | 4 | 5 | 1 | 2 | 3 | 0.25 | 0.33 | 0.5 | 0.25 | 0.33 | 0.5 | 1 | 1 | 1 | 3 | 4 | 5 |
| R34 | 0.33 | 0.5 | 1 | 1 | 2 | 3 | 0.25 | 0.33 | 0.5 | 0.25 | 0.33 | 0.5 | 0.25 | 0.33 | 0.5 | 1 | 2 | 3 | 1 | 2 | 3 | 0.33 | 0.5 | 1 | 0.2 | 0.25 | 0.33 | 0.2 | 0.25 | 0.33 | 1 | 1 | 1 |

System and information (R3) refers to the factors related to the functionality of the IoT system and the availability of information for the process. Four sub-criteria are identified: system reliability (R31), environmental data accuracy (R32), information security (R33) and system integration (R34). System reliability (R31) determines whether failure of the system would occur. Environmental data accuracy (R32) is a key factor in the electronic manufacturing process. The products involve chips, which are exposed to the air during the manufacturing, and is sensitive to temperature and humidity change. The quality of the products may vary with any environmental change, thereby increasing the defect rate. The temperature and humidity should be kept at standard conditions, for example, temperature 25°C and humidity 45%. Information security (R33) refers to the risks of the system being attacked by others and the data spread over the Internet. Since the manufacturing data is usually considered as confidential, the data collected by IoT should be securely stored in the cloud database. System integration (R34) is for considering if the implementation of IoT system would bring compatibility problem to the existing system in the company.

### B. *Pair-wise Comparison*

After identifying the key risk factors, the production manager and top managerial staff were interviewed to collect their opinions in electronic manufacturing risk management. Firstly, the opinion on the criteria (likelihood and consequence) in regard to goal was evaluated. Since there are sub-criteria in the 3-level hierarchy, pair-wise comparison was then conducted to evaluate the weighting of suddenly (C11) and occasionally (C12) likelihoods, as well as monetary value (C21) and time (C22), for consequence. Afterwards, the weights of each key risk factor were being compared based on the four sub-criteria. Table II shows an example of a fuzzy comparison matrix for alternatives to the sub-criteria (monetary value), with degree of fuzziness = 1. Taking breakdown of the facilities (R11) and workflow redesign (R12) as an example, it is found that the value of (4, 5, 6) is given by the company managers, which shows that the breakdown of the facilities (R11) is extremely important than workflow redesign (R12) when considering any financial loss suffered by the company. A sensitivity analysis is then conducted to determine the degree of fuzziness before generating the solution.

## V. RESULTS AND DISCUSSION

In this section, the research findings on sensitivity analysis, FAHP results and implications are discussed.

### A. *Discussion on Sensitivity Analysis*

In order to measure the degree of fuzziness, a sensitivity analysis is conducted to suggest how the ranking of criteria and risk factors will change. Let δ be the degree of fuzziness, where $\delta = u_i - m_i = m_i - l_i$, $0 \leq \delta \leq 1.9$. In the case study, δ is defined as 1 to generate the solution. Among the four sub-criteria, consequence (monetary value) (C21) is the dominant criterion when $\delta \leq 0.6$, which indicates that it is the most important when assessing the risk. After δ reaches 0.6, the likelihood (occasionally) (C12) has the next priority weight, while likelihood (suddenly) (C11) and consequence (time) (C22) follow. The sensitivity analysis of risk factors on the four sub-criteria are shown in Fig. 3 – Fig. 6. It is observed that the weight of risk factors converge when the degree of fuzziness increases.

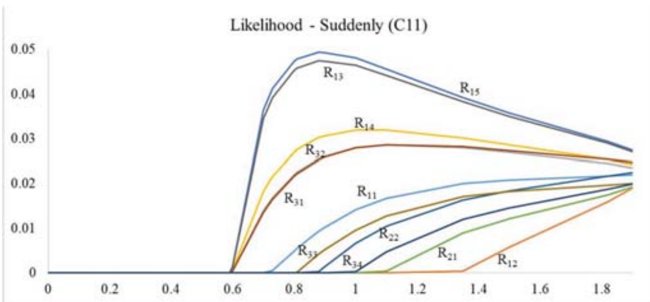


Fig. 3. Sensitivity Analysis of Risk Factors on Likelihood (Suddenly)

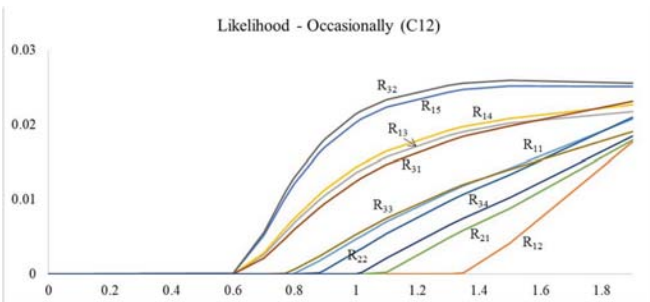


Fig. 4. Sensitivity Analysis of Risk Factors on Likelihood (Occasionally)

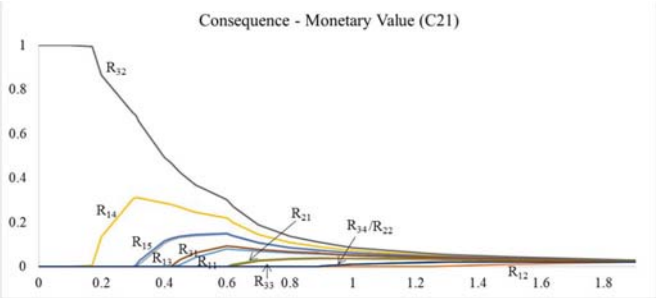

Fig. 5. Sensitivity Analysis of Risk Factors on Consequence (Money Value)

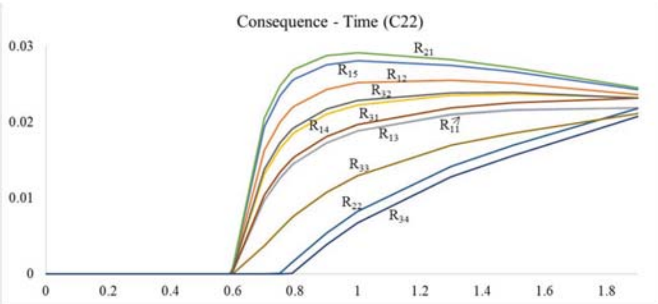

Fig. 6. Sensitivity Analysis of Risk Factors on Consequence (Time)

For likelihood (suddenly) (C11), as shown in Fig. 3, power failures (R15), unstable wireless internet network (R13), and improper operation (R14) have the highest weight when $\delta = 1$. However, the ranking changes when $\delta$ reaches 1.82. System reliability (R31) becomes the third priority in risk ranking. When $\delta$ reaches 1.35, it is found that all risk factors would achieve a positive weight.

For likelihood (occasionally) (C12), as shown in Fig. 4, environmental data accuracy (R32), power failures (R15) and improper operation (R14) have the highest weight when $\delta = 1$ . However, the ranking changes when $\delta$ reaches 1.83. System reliability (R31) becomes the third priority in risk ranking. In additional, it is observed that all risk factors have positive weight when $\delta$ reaches 1.35.

For consequence (money value) (C21), as shown in Fig. 5, it is found that environmental data accuracy (R32) is the dominant criterion when $\delta \leq 0.17$, which shows that it would bring serious consequence to money value if this risk occurs. It is because proper temperature and humidity are important in handling electronic products. The products would easily deteriorated if they are stored in improper environment, resulting in financial loss to the case company. When $\delta = 1$, improper operation (R14) has the next priority, followed by power failures (R15). The risk priority remain unchanged until $\delta = 1.9$. All risks achieve a positive value when $\delta \geq 1.24$.

For consequence (time) (C22), as shown in Fig. 6, resistance to change (R21), power failures (R15), and workflow redesign (R12) have the highest weight when $\delta = 1$. The risk priority remain unchanged until $\delta = 1.9$. In additional, it is observed that all risk factors have positive weight when $\delta$ reaches 0.79.

## B. Discussion on Findings

In this study, fuzzy logic is combined with AHP in risk analysis. Through the sensitivity analysis, it is found that the degree of fuzziness would affect the final result of risk priority. In this study, the degree of fuzziness is set between 0 and 1.9. Since consequence (monetary value) (C21) is the dominant criterion when $\delta \leq 0.6$, the weights for all risk factors in the other three sub-criteria, i.e. likelihood (suddenly) (C11), likelihood (occasionally) (C12), and consequence (time) (C22), are zero, indicating that they are less important when prioritizing the risk factors. In addition, it is found that some of the risk factors are excluded when the degree of fuzziness is set to be 1. Except consequence (time) (C22) in which all risk factors have positive weight when $\delta$ reaches 0.79, the degree of fuzziness of other three sub-criteria, i.e. likelihood (suddenly) (C11), likelihood (occasionally) (C12), consequence (money value) (C21) and consequence (monetary value) (C21) are too small to have a positive weight for all risk factors. All risk factors would have a positive weight when $\delta$ reaches 1.35, 1.35, 1.24 and 0.79 for C11, C12, C21 and C22 respectively. Therefore, the degree of fuzziness is set defined as 1.35, which is the maximum of the various minimum workable degree of fuzziness.

By following the FAHP steps discussed in the previous section and the result of sensitivity analysis, the normalized weighting after conducting pair-wise comparison is summarized in Table III, while the overall weights of key risk factors for each sub-criteria are shown in Table IV.

Fig. 7 shows the weights of the sub-criteria in the key risk factor prioritization. Among the four sub-criteria, it is found that monetary value (C21) in consequence has the highest weight among the four sub-criteria. Suddenly (C11) in likelihood and

TABLE III. NORMALIZED WEIGHTING AFTER PAIRWISE COMPARISON

| Criteria w.r.t. Goal | Sub-Criteria w.r.t. Criteria | Criteria Weighting | Alternatives w.r.t. Sub-Criteria |
|---|---|---|---|
| Likelihood (0.39) | Suddenly (0.61) | 0.24 | (0.08, 0, 0.11, 0.12, 0.16, 0.03, 0.06, 0.11, 0.16, 0.07, 0.05) |
| | Occasionally (0.39) | 0.16 | (0.07, 0, 0.12, 0.12, 0.15, 0.03, 0.06, 0.11, 0.16, 0.07, 0.04) |
| Consequence (0.61) | Monetary Value (0.61) | 0.37 | (0.09, 0.01, 0.11, 0.12, 0.11, 0.08, 0.06, 0.10, 0.14, 0.08, 0.05) |
| | Time (0.39) | 0.24 | (0.08, 0.10, 0.08, 0.09, 0.11, 0.11, 0.06, 0.09, 0.10, 0.07, 0.05) |

TABLE IV. OVERALL WEIGHTS OF KEY RISK FACTORS FOR EACH SUB-CRITERIA

| | C11 | C12 | C21 | C22 | Sum |
|---|---|---|---|---|---|
| **R11** | 0.020 | 0.012 | 0.037 | 0.021 | **0.090** |
| **R12** | 0.000 | 0.000 | 0.006 | 0.025 | **0.032** |
| **R13** | 0.028 | 0.019 | 0.041 | 0.021 | **0.110** |
| **R14** | 0.030 | 0.020 | 0.046 | 0.024 | **0.120** |
| **R15** | 0.039 | 0.025 | 0.042 | 0.027 | **0.133** |
| **R21** | 0.009 | 0.006 | 0.032 | 0.028 | **0.075** |
| **R22** | 0.016 | 0.011 | 0.022 | 0.015 | **0.064** |
| **R31** | 0.028 | 0.018 | 0.038 | 0.022 | **0.107** |
| **R32** | 0.038 | 0.026 | 0.051 | 0.024 | **0.139** |
| **R33** | 0.017 | 0.012 | 0.031 | 0.017 | **0.077** |
| **R34** | 0.012 | 0.007 | 0.021 | 0.014 | **0.054** |

time (C22) in consequence have the same weights, while Occasionally (C12) in likelihood has the lowest weight. The results show that the company is concerned whether the key risk factors would bring financial loss in IoT implementation.

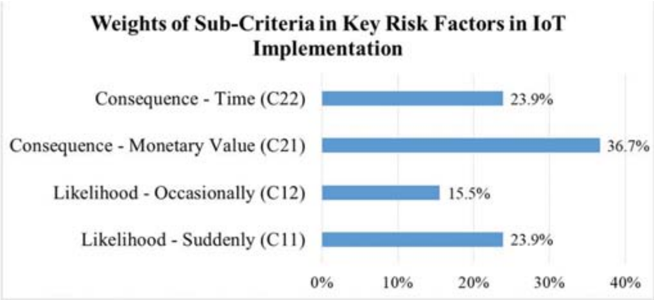


Fig. 7. Weights of Sub-Criteria in Key Risk Factors Prioritization

The overall weights of the key risk factors are shown in Fig. 8. It is found that environmental data accuracy (R32) has the highest priority in risk management with 13.9% weighting, followed by power failure (R15) and improper operation (R14), which have weightings of 13.3% and 12% respectively. Since electronic manufacturing involves environmental sensitive processes, both the temperature and humidity of work stations should be kept in a specific range. Any violation of temperature and humidity during the manufacturing process may make the electronic product deteriorate. The temperature and humidity data should be recorded in real time so as to ensure the quality of the product. Furthermore, instantaneous follow-up action can be made for any abnormal situation. Therefore, the accuracy of the environmental data is very important. It not only ensures the suitability of actual manufacturing environment, but also allows the implementation of instant follow-up action if a problem occurs. Power failure is the second highest risk for IoT implementation. It is because the adoption of IoT highly depends on a reliability electricity supply. The system may shut down if power failure occurs. The data cannot be collected and stored since the IoT system cannot be operated without power.

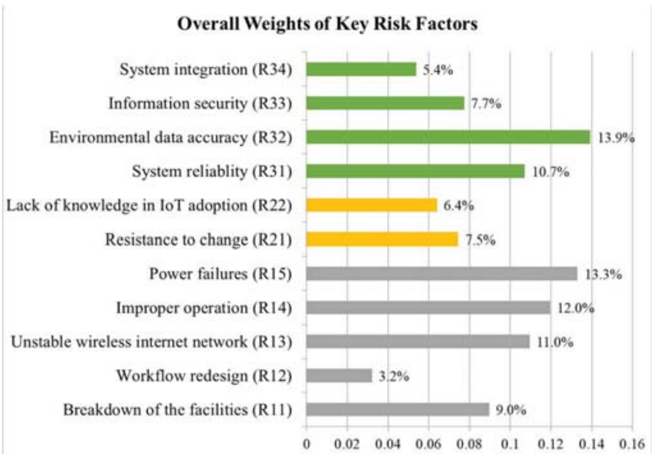


Fig. 8. Overall Weights of Key Risk Factors

### C. *Discussion on Implications*

After implementation of the EM-RMM, the changes in the company are visible in three areas: decision making process, strategic solution, and time for decision making. It implies that the proposed model is capable to manage risk factors by considering multiple criteria in a systematic approach.

#### 1) *Decision Making Process*

Before the implementation of the EM-RMM, decisions were made rather arbitrarily with only management's personal experiences and observations as reference. There were no standard processes of risk management. The EM-RMM offers a systematic mean of risk management in the case company. The flow of implementation of the EM-RMM is discussed in detail, with step-by-step instruction for different phases and different stages. The EM-RMM is divided into two phases; each with a specific purpose to achieve the goal of selecting the key risk factors and formulating a solution around these risk factors.

#### 2) *Strategic Solution*

Before implementation, there was no strategic solution for risk. With EM-RMM, a targeted strategic solution was developed based on the causes and features of the key risk factor. Since the risk factor was selected through weighing the importance of several criteria by management, the risk factor not only reflects challenges in the operational aspect, but also the strategic aspect. The strategy was developed by adopting risk treatment principles and taking the root cause of the risk factor into consideration in the development, instead of only focusing on the effect of the risk. Therefore the solution is more effective in the long term.

#### 3) *Time for Decision Making*

Before implementation, the company needed to find and collect information for risk management from different departments. A long period of time was needed for manual information collection. The EM-RMM collects the data and store them in a centralized database, saving time and effort in making managerial decisions.

## VI. Conclusions

By reviewing the past literature, it is found that an IoT-based solution brings significant changes to the manufacturing processes. It provides an efficient and reliable network which increase information visibility and fast problem detection for timely decision making. Although the implementation of IoT-based solution can provide benefits in manufacturing processes, limited attention has been paid on how to implement IoT smoothly by considering risk concerns. In this study, an electronic manufacturing risk management model (EM-RMM) is presented by applying FAHP in risk management. Based on two criteria (i.e. likelihood and consequence), eleven potential key risk factors regarding IoT implementation in three areas (i.e. operations, labor, and, system and information) are identified. This approach not only considers multiple criteria in risk evaluation, but also transforms the fuzziness of managerial preference into measurable values for decision making. Since risk management is a continuous process, further study will be undertaken on risk management during the implementation process for continuous improvement.

## ACKNOWLEDGMENTS

The authors would like to thank the Engineering Doctorate Programme, Faculty of Engineering of The Hong Kong Polytechnic University for inspiring the development of this project.

## REFERENCES

[1] H. S. Kang, J. Y. Lee, S. Choi, H. Kim, J. H. Park, J. Y. Son, B. H. Kim, and S. Do Noh, “Smart manufacturing: Past research, present findings, and future directions”, Int. J. Precis Eng Manuf-Green Technol., vol. 3(1), pp. 111-128, 2016.

[2] J. S. Randhawa, and A. S. Sethi, “An Empirical Study to Examine the Role Smart Manufacturing in Improving Productivity and Accelerating Innovation”, Int. J. Eng. Manag. Res., vol. 7(3), pp. 607-615, 2017.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, Futur. Gener. Comp. Syst., vol. 29(7), pp. 1645-1660, 2013.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications”. IEEE Commun. Surveys Tuts., 17(4), pp. 2347-2376, 2015.

[5] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, “Information-centric networking for the internet of things: challenges and opportunities”, IEEE Netw. vol. 30(2), pp. 92-100, 2016.

[6] M. B. Kearns, J. B. Taylor, and C. E. Hull, “The six facets model: technology management in the effective implementation of change”, Int. J. Inno. Tech. Manag., 2(1), pp. 77-100, 2005.

[7] Y. Sun, H. Song, A. J. Jara, and R. Bie, “Internet of things and big data analytics for smart and connected communities”, IEEE Access, vol. 4, pp. 766-773, 2016.

[8] F. Wortmann, and K. Flüchter, “Internet of Things”, Bus. Inf. Syst. Eng., vol. 57(3), pp. 221-224, 2015.

[9] F. Shrouf, and G. Miragliotta, “Energy management based on Internet of Things: practices and framework for adoption in production management”, J. Clean Prod., vol. 100, pp. 235-246, 2015.

[10] X. V. Wang, and L. Wang, “A cloud-based production system for information and service integration: an internet of things case study on waste electronics”, Enterp. Inf. Syst., vol. 11(7), pp. 952-968, 2017.

[11] F. Tao, J. Cheng, and Q. Qi, “IIHub: An Industrial Internet-of-Things Hub Toward Smart Manufacturing Based on Cyber-Physical System”, IEEE Trans Ind. Informat., vol. 14(5), pp. 2271-2280, 2018.

[12] M. Giannakis, and T. Papadopoulos, “Supply chain sustainability: A risk management approach”, Int. J. Prod. Econ., vol. 171, pp. 455-470, 2016.

[13] A. Fertis, M. Baes, and H. Lüthi, “Robust risk management”, Eur. J. Oper. Res., vol. 222(3), pp. 663-672, 2012.

[14] B. G. Hwang, X. Zhao, and L. P. Toh, “Risk management in small construction projects in Singapore: Status, barriers and impact”, Int. J. Proj. Manag., vol. 32(1), pp. 116-124, 2014.

[15] O. Taylan, A. O. Bafail, R. M. Abdulaal, and M. R. Kabli, “Construction projects selection and risk assessment by fuzzy AHP and fuzzy TOPSIS methodologies”, Appl. Soft. Comput., vol. 17, pp. 105-116, 2014.

[16] J. Oehmen, A. Olechowski, C. R. Kenley, and M. Ben-Daya, “Analysis of the effect of risk management practices on the performance of new product development programs”, Technovation, vol. 34(8), pp. 441-453, 2014.

[17] Y. Grushka-Cockayne, S. Erat, and J. Wooten, “New Product Development and Project Management Decisions”, in The Handbook of Behavioral Operations, K. Donohue, E. Katok and S. Leider Eds., N.J.: Wiley 2018, pp. 367-392.

[18] S. M. Neves, C. E. S. da Silva, V. A. P. Salomon, A. F. da Silva, and B. E. P. Sotomonte, “Risk management in software projects through knowledge management techniques: cases in Brazilian incubated technology-based firms, Int. J. Proj. Manag., vol. 32(1), pp. 125-138, 2014.

[19] M. M. D. Carvalho, and R. Rabechini Junior, “Impact of risk management on project performance: the importance of soft skills”, Int. J. Prod. Res., vol. 53(2), pp. 321-340, 2015.

[20] S. Marcelino-Sádaba, A. Pérez-Ezcurdia, A. M. E. Lazcano, and P. Villanueva, “Project risk management methodology for small firms”, Int. J. Proj. Manag., vol. 32(2), pp. 327-340, 2014.

[21] P. Akhtar, Z. Khan, S. Tarba, and U. Jayawickrama, “The Internet of Things, dynamic data and information processing capabilities, and operational agility”, Technol. Forecast. Soc. Chang., vol. 136, pp. 307-316, 2018.

[22] J. E. Kim, T. Abdelzaher, L. Sha, A. Bar-Noy, R. Hobbs, and W. Dron, “On maximizing quality of information for the internet of things: A real-time scheduling perspective”. 2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), IEEE, pp. 202-211, 2016.

[23] M. Ilangkumaran, M. Karthikeyan, T. Ramachandran, M. Boopathiraja, and B. Kirubakaran, “Risk analysis and warning rate of hot environment for foundry industry using hybrid MCDM technique”, Saf. Sci., vol. 72, pp. 133-143, 2015.

[24] T. L. Saaty, “How to make a decision: the analytic hierarchy process”, Eur. J. Oper. Res., vol. 48(1), pp. 9-26, 1990.

[25] X. Wang, H. K. Chan, R. W. Yee and I. Diaz-Rainey, “A two-stage fuzzy-AHP model for risk assessment of implementing green initiatives in the fashion supply chain”, Int. J. Prod. Econ., vol. 135(2), pp. 595-606, 2011.

[26] S. A. T. Khodadadi, and B. D. Kumar, “Contractor Selection With Risk Assessment By Using AHP Fuzzy Method”, Int. J. Adv. Eng. Technol., vol. 5(2), pp. 311-318, 2013.