A new criticality analysis approach for infrastructure components

NEW FMECA APPROACH FOR INFRASTRUCTURE ASSET MANAGEMENT

Ragavendar Ganesh | CME2000 Master thesis

ஒருமைக்கண் தான்கற்ற கல்வி ஒருவற்கு
எழுமையும் ஏமாப் புடைத்து.

குறள் எண்: 398

Colophon

AUTHOR DETAILS

Name	R.T. (Ragavendar Thrivikram) Ganesh
Student number	4746775
E-mail	ragvik61@gmail.com
Contact number	+31 6 262 715 09

GRADUATION COMMITTEE

Chairman	Prof. Dr. Ir. R. (Rogier) Wolfert Faculty of Civil Engineering and Geosciences (CiTG)
Supervisor	Ir. M. (Martine) van den Boomen Faculty of Civil Engineering and Geosciences (CiTG)
Supervisor	Ir. J. (Jeroen) Hoving Faculty of Civil Engineering and Geosciences (CiTG)

GRADUATION THESIS

University	Delft University of Technology
Faculty	Civil Engineering and Geosciences (CiTG) Stevinweg 1, 2628 CN Delft
Master	Construction Management and Engineering (CME)
Course	CME2000 Graduation Thesis

“Learning acquired once will stand in good stead forever.”
Thirukkural Nr.398

Acknowledgements

I take this opportunity to heartfully thank my committee members for giving me the chance to take up such a challenging research. I thank my chairperson, Dr. Ir. Rogier Wolfert for his unique critical observation on my research. His guidance instigated me to keep pushing myself to the fullest of my potential. Following his support, I take an immense pleasure in expressing gratitude to my first supervisor, Ir. Martine van den Boomen, who gave her utmost support and encouragement throughout my entire thesis work. Her distinctive guidance and eye for detail on my works were extremely helpful, without which, writing a research article would still be a dream for me. Then, I'd like to thank Ir. Jeroen Hoving for his timely supervision on the critical points of my research, helping me sharpen my skills in writing and presenting my works. Their constant analytical view and constructive feedbacks helped me bring out a worthy contribution to this field of study.

I thank the entire CME fraternity for their support at various stages of my study, especially my batchmates without whom my master's degree at TU Delft wouldn't have been this pleasurable. A special thanks to my closest folks, Padmapriya Arulkumar, Getssy Prathiba, Athithya Vemuri, Rahul Ramesh, and Avin Shanbag for their constant motivation and support all along this thesis journey. Finally, I would like to thank my parents, sister and grandparents for their constant support during my entire thesis. Although at a distant, they still made sure my life was a lot easier in the past months.

As a token of gratitude towards my land of origin,

“என் தாய்யிற்கும் என் தாய் மண்ணிற்க்கும் சமர்ப்பணம்”

I hope you enjoy reading this report!

Ragavendar Thrivikram
Delft, The Netherlands

Executive summary

This report is a result of my graduation research which was completed as a part of the coursework CME2000 Master thesis. This thesis work has helped me understand the nuances of independent research and what it takes to solve a problem scientifically. This work was a steep learning curve to understand how proven theories and concepts can solve new issues by a contemporary application. This thesis attempted in develop a new risk assessment approach for infrastructures using FMECA. The current research endeavours with an ultimate goal of developing an approach that can provide reliable inferences to develop optimal maintenance strategies. This report provides an extensive problem description and a lay-downs a research design implemented to solve the issue identified. Based on the problem and scope of research the main research question framed is as follows,

"What is an optimal risk assessment approach in FMECA to obtain accurate criticalities of repairable components present in an infrastructure system?"

The developed method uses a range of quantitative data derived from a standardized system reliability and availability calculations. The derived data was incorporated in a state-of-art risk matrix design identified from a critical literature analysis. An added value of the current research is it's improvement of the existing FMECA technique. For validation, the developed method was applied on two infrastructure systems along with the conventional method for a comparative analysis. From this analysis it was evident that the new method gave better quantitative inferences than the conventional method. Thus, solving the primary objective of research and the problem identified successfully. As a result, a research paper targeting professional journals would be submitted for publishing in the coming days. The research paper written is added to this report for the research's content description.

Management summary

The chosen Master Thesis project is associated to the fields of infrastructure asset management, drawing a specific study towards the maintenance optimisation. This report presents the graduation thesis in a report form for the CME2000 Master Thesis coursework. This section of the report provides an elaborate summary of the research, covering a brief introduction to the identified problem and what exactly the research endeavours on. The research questions framed for the problem description are provided. And finally, a hint on how the solution identified solves the issue is explained.

In general, for any infrastructure system, its availability and operational reliability lies with how effective the risks associated to its components are analysed. Therefore, accuracy of risk assessments is vital for developing effective measures to reduce their effects upon occurrence. The same principle applies while developing maintenance plans for any infrastructure using different risk assessment techniques. Among the many methods used for risk assessments, when it comes to maintenance planning, the failure mode effect and criticality analysis (FMECA) stands tall in the list of highly used techniques. Within FMECA the criticality (or) risk levels of each component is analysed using a risk matrix.

Given its high range of industrial application, FMECA still has major limitations because of its qualitative attributes. These attributes affect the way risk matrices are applied to assess criticalities. What are the problems with its application? A major problem with risk matrices is that they are designed from the perspective of a system and applied to assess components. This makes the risk matrices to neglect the uniqueness of each component within the system. The errors in design and type of inputs used in risk matrices affect its analysis on components and provides inaccurate and off-scale results. The design issues with risk matrices causes risk reversal errors, improper judgements and extreme results. Importance of a risk matrix in maintenance is an understatement since intervention actions for each component is based on its position in the risk matrix. Hence, due to involvement of such issues, the developed maintenance plans become less reliable.

The following paragraphs provide practical insights on how the above-mentioned limitations affect a FMECA's industrial application. In practice, a governmental organization or a firm (asset owner) tenders out an infrastructure project. The tender proposals of contractors are judged based on how they meet with the performance requirements set out by an asset owner. To check if the components and their designs provided by contractors comply to the requirements, a system's risk matrix is used. As mentioned earlier having a system risk matrix to check components neglects their uniqueness. To check if a contractor's design complies to the required operational reliability, we need a risk matrix that could account failures of components and their compiled effect to the system. This limitation in risk matrices used in FMECA makes its application ineffective.

To increase accuracy of maintenance plans, use of quantitative data is highly recommended. Since the conventional risk matrix and FMECA method involves the use of different qualitative assumptions, the current research attempts in extending this technique using a range of unique quantitative inputs. These inputs must be derived from a reliable process and provide information on the components and its compiled effect on the system. From an initial literature search, an existing research gap on the problem identified was experienced. Hence, making this research have a novelty in its content

The current research uses standard system reliability and availability (RA) calculations to derive the required quantitative data. Since infrastructure components in general are repaired upon failure, the RA calculations are done assuming a certain maintenance strategy. Therefore, for the solution expected to the solve the issue in hand the following sub-research were framed,

Sub-research questions

(i) Which risk matrix design suits best for analysing components and subsystems?
(ii) What is the standardized procedure to perform RA calculations for repairable systems based on IEC 61708 norms?
(iii) How can interdependencies and importance's of each component within a system be determined?
(iv) What is the best possible incorporation of obtained quantitative inputs for risk assessment in FMECA?
(v) How can the risk matrix designed from a systems' perspective provide criticalities of components and subsystems?

A pragmatic research strategy to facilitate both quantitative and qualitative study was implemented. The research methodology to be followed is sketched and works involved in each phase is delineated as shown in chapter 3 of this report. From this juncture the research endeavours in identifying an appropriate risk matrix design and quantitative data to assess components.

Upon research an iso-risk based risk matrix design was chosen for application. The acceptability limits of the risk matrix were set using the performance requirements of systems so that components can be assessed based on their compliance to the system needs. This eliminates the major issue of applying a system's-based risk matrix on components directly. From the RA calculations, various quantitative inputs that provides a numerical interpretation on the component's state in the system is studied. From the obtained quantitative data, it was possible to define a component based on its (i) conditional failure rate and (ii) importance to the system using Vesely's conditional failure rate and a so-called Lambert's importance factor. These factors when incorporated appropriately provided better inputs for the risk matrix to obtain accurate component criticalities.

To ensure appropriate use of risk matrices and the quantitative data obtained, a well-delineated methodology was developed. The developed methodology depicts the way this new approach checks a system's compliance to the performance requirements and the component's criticality in the system. An extension to the conventional risk interference is developed, in such a way the risk matrices prioritise components based on their importance and impacts. To validate the developed methodology, application on two case studies along with the conventional method was done for a comparative analysis. From the results obtained, it was evident that the new method provides better quantitative insights to derive accurate criticalities of components. From the results obtained, answering the main research question was possible. The main research question is as given below,

"What is an optimal risk assessment approach in FMECA to obtain accurate criticalities of repairable components present in an infrastructure system?"

The different discussions and recommendations for the obtained results are provided in this report. For the novelty of this extension to the FMECA technique, the thesis resulted in writing a standalone research article. This research paper forms the content description in this report. Overall the report provides a detailed thesis outline on the problem identified and research design. Additional illustrations to support the research paper are provided. The works were carried out successfully and the final stages of the thesis focused majorly towards perfecting the paper.

Table of Contents

Table of Figures

This page was left blank intentionally

Chapter 1. Introduction

Infrastructures are the basic requirement for a country's economy development, employment, healthcare, mobility, education, aesthetics and livelihood requisites. These constructions are not only targeted towards the improvement in 'Quality of Life', but are also used as protective structures from natural calamities such as floods, hurricanes, tsunamis etc (Aschauer, 1990). In recent times, infrastructures play a major role in the modern world to bolster the constant growth in development of science and technology. For these very reasons, a wide-range of investments to construct complex and innovative structures are being made. Many infrastructure projects are being initiated around the world and countries include such investments as a part of their development goals. Case in point, this can be seen from the UN and Asian countries' initiatives, where development goals have been established to invest tens of trillions of dollars on new infrastructures ranging from roads, mines, and hydroelectric dams (Laurance et al., 2015). These initiatives are easily spottable among the developing countries. Having affiliation towards such investments can help them in terms of revenue and several other socio-economic factors.

For every infrastructure project, following its completion the challenge of maintaining them for a longer lifespan becomes elemental. As we know, infrastructures in general, are high-priced investments and their failures cause major damages in terms of economy, safety and environment to both asset owners and the public. Hence, a primary prerequisite for any asset owner (e.g. governmental bodies, private investors), is maximum availability of their infrastructures with minimal failures. Several construction enterprises are actively investigating new strategies and methods to obtain longer lifespans of infrastructures, to extract its maximum benefits. One of the most commonly adopted strategy across all construction firms is to have a specialized asset management team (Rajeev Ruparathna, Kasun Hewage, 2017). This team works on identifying solutions through extensive risk assessment, reliability analysis etc. to identify critical components of an infrastructure.

Among all solutions, effective maintenance to extract maximal functionality of an infrastructure project has become the best approach to satisfy requirements of an asset owner (Arunraj & Maiti, 2007). Having a comprehensive maintenance, can improve an infrastructure's lifetime and at the same time ensure a higher availability each year. Since failures of infrastructures depend on how well their composite components are maintained, a wide-range of research is being held in this field. The maintenance interval and repair rates of component depend upon the type of (sub)system (series, parallel, redundant) they are present in (Giorgio, M., & Mohamed, 2014). The aim of maintenance is to lessen the effect of risks posed by components on reducing its likelihood or impact upon failure (Yusta, Correa, & Lacal-ara, 2011). The principle used for developing maintenance strategies work similar to risk management planning done for different phases of a project. This is explicitly seen in most infrastructure projects where an all-encompassing risk assessment of components is done to develop several maintenance strategies.

The commonly adopted technique to analyze criticality of each component present within a system is the Failure mode effect and criticality analysis (FMECA) method (Kapadia & Llc, 2017). In the field of Infrastructure asset management, FMECA is widely used for the purpose of developing maintenance plans. To maintain an infrastructure efficiently, we need information on how components are assembled in them. Considering an infrastructure as a system, aids in obtaining a better visualisation of its internal (components) build. Such picturing helps in identifying the different possible failure combinations that can occur and its respective effects on the system. The FMECA technique helps in identifying the different failure modes of each component and its effect to the system. Additionally, this technique also analyzes the criticality (or) risk level of each component in the system (IEC 31010, 2018).

Infrastructures are made up of several components and subsystems. Each component has its own failure frequency by design and downtime (repair) required to bring them back to a functioning condition. While developing maintenance plans, prioritizing components and subsystems based on their criticalities help in aligning maintenance interventions. A risk (or) criticality of a component depends on the mean time between failure ($MTBF$) and its mean downtime (MDT). In FMECA, a conventional risk interference ($Risk = MTBF * MDT$) is followed for assessing a component's criticality. On plotting the interferences in a risk matrix, components are ranked and prioritized based on its position.

Although FMECA provides the required inferences to develop maintenance planning it relies majorly upon qualitative inputs. A major limitation of using such inputs is that it brings down the accuracy of risk assessments. Risk matrices using qualitative inputs to assess each component and subsystem neglects the relation and position in the system it exists in. A component's position in a system depends on (i) the number of similar components present, (ii) its configuration and (iii) conditional failure rate. The negligence occurs in FMECA since, components are analyzed individually without accounting for its position within the system. Adding to this, errors associated to the RM also cause off-scale and off-categorization results. One of the major problems with the RM occurs since they are designed from a system's perspective although they are applied to and assess components in it.

The current research ventures with a primary objective of achieving accurate maintenance plans. For which the existing FMECA approach, widely used for developing such plans is endeavored to be improved of its accuracy. To do so, the identified drawback must be resolved. To overcome this limitation, we require unique quantitative indicators of components accounting for the above-mentioned factors. With such indicators we can derive a much better risk assessment of components based on their relation and position in the system. To obtain the required quantitative information of each component, the current research uses a standard reliability and availability (RA) analysis.

In order to incorporate the obtained indicators, the research entails in developing a new risk assessment approach for FMECA using RA analysis. The conventional RA analysis is done assuming that upon failure, each component is replaced with a new one. But since we deal with infrastructures where upon failure each component is repaired and brought back either (i) to a good as new condition or (ii) a minimal repair is done to bring them back to its previous working condition (Ebeling, 2005). Hence, the impact faced when a component fails is the downtimes incurred during the repair period. The current research accounts for the repairability of components under a certain maintenance strategy.

The main objective here is to improve the accuracy of risk assessment of components in the system level and in turn extend the quality of maintenance planning. Hence this research attempts in developing a new approach comprising changes to the conventional RM used and the inputs for judging criticalities. The developed approach is aimed to be applied on infrastructure systems along with the conventional method to obtain a comparative analysis on the results obtained.

The report's outline is as follows. Chapter 2 provides a detailed description of the problem identified with a short example. Based on which, chapter 3 provides a broad research strategy based on objectives of research and solutions required to solve the problem under scrutiny. In addition, a detailed methodology framed for the research is provided. Chapter 4 consists of the research paper showcasing the current research work and a case study. Thereof, chapter 5 provides supplementary illustrations on methodology developed and an additional case study. Chapter 6 follows with conclusions being made from the research.

Chapter 2. Problem statement

This chapter presents a detailed explanation of the problem identified in the risk assessment of FMECA. Initially a general description of the problem is provided. Following which a detailed illustration using an example is shown to validate its existence in practice. Finally, a brief explanation on how this problem affects maintenance planning is given.

2.1 PROBLEM DESCRIPTION

Infrastructures can be considered as repairable systems comprising several individual components and subsystems. Components existing as subsystems cannot be considered similar to individual components. This is because, subsystems usually comprise of several similar or diverse components arranged in a particular configuration (for e.g. serial, parallel, bridge, etc.). Such components fail at a unique conditional rate based on the type of configuration. And the impact posed by such components depend upon their importance within the system. For example, a component existing as a serial subsystem would have a higher importance to the system. Since upon failure of a single component, the entire subsystem fails. Whereas, components existing as a parallel subsystem will have a low importance since they fail only upon failure of all components (Ebeling, 2005). Sometimes in certain systems few components have more than one of its similar kind at different locations rather than existing as subsystems. Hence, while assessing risks of such components their position and importance to the system must be considered.

However, in an FMECA technique, the different failure modes of each component are analyzed individually. By doing so, their risks are analyzed without considering their position and importance in the system. Thereof, a limitation exists in the way risks are assessed in an FMECA. Hence a component's position in a system depends on three major factors, (i) number of similar components and the type of configuration, (ii) its typical failure rate (for individual components) or conditional failure rate (for subsystems) and (iii) its importance in the system. Only on analyzing each component based on these factors we can obtain its accurate risk value and criticality to the system.

In a typical FMECA, criticality of components are analyzed based on their failure modes and effect. The risk matrix plots each component based on their mean time between failures ($MTBF$) and mean downtime (MDT). The following section provides an illustration of the problem described in the previous paragraphs.

2.2 PROBLEM ILLUSTRATION

For the purpose of simple interpretation, a straightforward system consisting of 4 similar components as shown in figure 1 is chosen. To get an interpretation of the problem, risks of each component is assessed based on two scenarios, (i) considering it to be individual and (ii) considering its position.

Assumptions:

The system has a serial configuration consisting an individual component and a subsystem as shown in Figure 1. The basic component information is as given below,

Component A exists individually in the system and has a typical failure rate, $\lambda_{c_A} = 1.1^{-4}$ or $MTBF_A\left(\frac{1}{\lambda_{c_A}}\right) = 1\ year^{-1}$ and $MDT_A = 2$ hours.

Component B exists as a subsystem with a parallel configuration consisting of 3 similar components. Each component (B_1, B_2 and B_3) fails at a similar $\lambda_{c_{B_i}} = 1.1^{-4}$ or $MTBF_{B_i}\left(\frac{1}{\lambda_{c_{B_i}}}\right) = 1\ year^{-1}$ and has an impact or $MDT_{B_i} = 4$ hours.

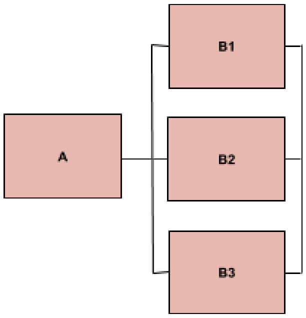

Figure 1 System decomposition

(i) When we assess components individually (Conventional method)

As we can see from the system decomposition, two components A and B are present in a serial system, where B exists as a parallel configuration of 3 similar components. In a conventional FMECA, we assess each component individually based on their $MTBF_i$ and MDT_i as shown in Table 1. Now, from the risk values obtained it is seen that component B has a quantitatively higher risk in the system than A. Hence, maintenance intervals are prioritized such a way that actions for component B should precede than those for A. From this assessment we conclude that component B is more critical than component A.

Table 1 Conventional risk assessment

Components	$MTBF_i$ ($year^{-1}$)	MDT_i (hours)	$Risk_i$
A	1	2	2
B	1	4	4

(ii) When we assess components considering their position

To understand the position of a component in a system, analysing the (i) type of configuration (ii) number of similar components and (iii) conditional failure rate is required as mentioned in the previous section of this chapter. From the system decomposition (figure 1), it is evident that component B exists as a parallel configuration. Hence, we can understand that only upon failure of all the similar components (B_1, B_2 and B_3) present in the subsystem, B fails. This failure event where all 3 similar components losing function will have a higher $MTBF$ (or) lower failure rate than the individual rate ($\lambda_{c_{B_i}}$). Whereas, the component A will have the same $MTBF_A$ and MDT_A since it fails at its own rate without any dependencies. Hence, we can now say that the risk of A is much higher than that of B while considering a component's position and importance in the system. Therefore, intervention actions for B can be delayed and whereas A requires a more stricter maintenance action.

2.3 PROBLEM ANALYSIS

From the problem illustration, we can see how overlooking a component's position and importance in the system can cause contrasting component criticalities. Criticalities of components play a vital role in prioritizing maintenance actions. Errors in the way we determine these criticalities affect maintenance strategies to a great extent. Overlooking the position held by components, sometimes overestimates risks of less critical components resulting causing excess maintenance investments. And also, vice versa, where certain critical components are assessed as non-critical causing unforeseen failures.

These errors are not only caused due to the limitation of individually assessing components in FMECA but are also caused by the application of risk matrix. An inaccurate risk value obtained from an erroneously designed risk matrix makes the maintenance plans less reliable. Hence using an appropriate type and design of a risk matrix is important. The various errors of risk matrices are explained from the point of a critical literature analysis in the research paper (Chapter 4). To eliminate the issues identified from this analysis, an extensive search on available design methods can help in identifying an appropriate design for assessing such infrastructure systems.

The other major issue as explained earlier is associated with the risk matrices is its application or design from a system's perspective. These risk matrices are then applied on components to check its criticality to the system. The problem of using such risk matrices, a components contribution to the system's loss of function is missed. Thus, a risk matrix neglects the fact that each component within the system has a unique effect depending upon its positional importance. Sometimes different risk matrices for distinct levels of functional losses are designed and combined to a single matrix. But even on doing so, a constant acceptability limit continuing for each level of functional loss is difficult to be included. Apart from the acceptability limit, to assess a component's contribution to the level of functional loss has to be done qualitatively. Although human biases come into play, still risk matrices are only designed for a range of functional losses. Only on using system-specific acceptability limits and quantitative inputs, compliance check of components to the system's requirements can be done. And based on their compliance state, we can define its criticality to the system. Due to this negligence, erroneous results (off-scale and off-categorization) are obtained for components that are non-individual or non-independent.

The current research endeavors in solving the problems identified in the previous paragraphs using a set of quantitative data for risk assessments. Thereof, maintenance plans must be developed using quantitative data for each component in a system. Using such data would reduce the presence of human biases and procedural errors in maintenance plans (Memarzadeh & Pozzi, 2016a). To assess if a component is critical we need quantitative inputs / importance in the system. Given the fact that infrastructures are built up of several components and subsystems, their maintenance actions should be prioritized based on their importance to the system. With the required quantitative data and a suitable risk matrix designed using system specific limits, can remove the problems identified in FMECA. In addition, on incorporating indicators providing a component's importance, a well prioritized maintenance planning can be developed.

To obtain the required risk matrix and quantitative data and the following chapter entails a design of research strategy that would aid in solving the identified problem.

SUB-CONCLUSION

The problem identified with the FMECA caused due to the limitations present in the way risk matrices are applied for risk assessment is described and delineated in this chapter. To showcase an illustration on the problem identified, a simple system decomposition with basic assumptions was used. From the analysis of the problem we can conclude saying the limitation with FMECA is that the risk matrices neglect the position and importance of components present in the system. Hence, we require quantitative information that can account for (i) number of similar components, (ii) type of configuration and (iii) importance in the system. The following chapter design a research strategy that would aid in obtaining the desired results without deviations.

Chapter 3. Research design

To ensure a stable course of research on the problem identified and with no deviations in goals, a research design is prepared to aid in obtaining required results. This chapter initially provides the scope and different objectives of the current research. Following which the different sub-research questions and the main research question is framed based on the problem analysis in the previous chapter. Finally, a research methodology sketching the different phases for solving the framed questions are explained in detail.

3.1 SCOPE OF THE RESEARCH

Among the different fields of study related to infrastructure management, the current research revolves around its maintenance. With the development of innovative construction techniques and tools bringing complex infrastructures into reality has become a conceivable affair. The costs budgeted for maintenance actions stands next to the energy costs of the operational budget of an infrastructure (Dekker, 1996). Hence, the most concerning fields of research deals with identifying solutions to obtain optimal maintenance strategies for such infrastructures.

In every infrastructure project, assessing the various risks involved in different phases until its maintenance to develop mitigation measures of great importance (Arunraj & Maiti, 2007). On analysing the different risks, various mitigation measures and strategies are developed to reduce their possible effects. Failures of infrastructures result in immense financial losses. The principles of risk management are similar to what is being followed for maintenance planning. Among the several standardised risk assessment techniques available, the most widely used technique for maintenance planning is the failure mode effect and criticality analysis (FMECA). With the scope narrowed down and problem identified, the current research would focus upon solving the limitation that exists in the risk assessment of the FMECA technique. The research is carried out with an ultimate aim of improving the existing technique to devise optimal maintenance strategies.

Since the research requires quantitative information to improve the conventional risk assessment. This study uses standardized reliability and availability (RA) calculations considering infrastructures as repairable systems. The calculations are performed based on the equations and IEC 61708:2016 norms for Reliability block diagrams. The case studies used in this research are real-time infrastructure systems with basic assumptions for a lucid interpretation of the developed method.

3.2 RESEARCH OBJECTIVE

The primary objective of the research is to develop an improved risk assessment approach that accounts for a component's interdependency and position within the system. The new approach must comprise of, unique quantitative inputs from reliable process and calculations to provide accurate criticalities and prioritization. Since maintenance strategies depend majorly on criticalities of components, an understated objective of this research is to improve the risk matrix using an appropriate design and quantitative inputs. On doing so, an added value of the research is developed an improved FMECA technique that could devise optimal maintenance plans.

From a deliverable's point of view the objectives are to obtain, (i) a state-of-art risk matrix design that can eliminate the errors incurred in a conventional method, (ii) quantitative inputs from system calculations for a better risk assessment and (iii) a detailed procedure to implement the developed approach.

3.3 SCIENTIFIC CONTRIBUTION

A line of reasoning for the scientific contribution of this research rises from the discussion made, to whether downgrade the risk matrix tool in the forthcoming update of ISO/IEC 31010 Risk assessment techniques standards, to a reporting technique (Peace, 2017). Although risk matrices don't provide the most accurate results it still has a wide-industrial application. Lack in understanding the concepts associated with each type of risk matrix is the reason for its downfall. The current research provides a novel approach for applying risk matrices to assess infrastructure components. This adds significance to existing application of risk matrix in the FMECA technique, making it become a powerful tool in the field of risk and infrastructure asset management.

3.4 RESEARCH QUESTIONS

Based on the problem stated and objectives defined, this section provides the different sub research questions following by the main research question.

3.4.1 Sub-research questions

(a) Which risk matrix design suits best for analysing components and subsystems?
(b) What is the standardized procedure to perform RA calculations for repairable systems based on IEC 61708 norms?
(c) How can interdependencies and importance's of each component within a system be determined?
(d) What is the best possible incorporation of obtained quantitative inputs for risk assessment in FMECA?
(e) How can the risk matrix designed from a systems' perspective provide criticalities of components and subsystems?

3.4.2 Main Research Questions

"What is an optimal risk assessment approach in FMECA to obtain accurate criticalities of repairable components present in an infrastructure system?"

3.5 RESEARCH METHODOLOGY

Following the questions framed in the previous section, a research methodology delineating the different phases of the study is explained. This section delineates the method outline giving a visualisation on the research flow and how each phase answers the questions framed. The methodology comprises of a pragmatic approach since a combination of qualitative and quantitative study is involved for the current research. Since we require inputs from different techniques and concepts, multiple angles of arguments are required to obtain a greater evidence-better argument approach (Saunders, Lewis, & Thornhill, 2012). The research does not stop with a new method development, but also applies it to two infrastructure systems. Since the current research attempts to validate the effectiveness of developed method against the conventional method, a comparative case study strategy is followed (Verschuren, Doorewaard, Poper, & Mellion, 2010). The methodology consists of five major phases, (1) Scientific review on literatures of RM and a technical study on standard RA calculations for repairable systems, (2) Data collection for case studies, (3) Performing quantitative analyses on the cases obtained, (4) Comparative analysis (New approach vs Conventional method) (5) Development of a step-wise procedure sketch for the new approach. Since each of these phases comprise both quantitative and qualitative works, a pragmatic approach is applied in each step of the research.

3.5.1 Phases of research

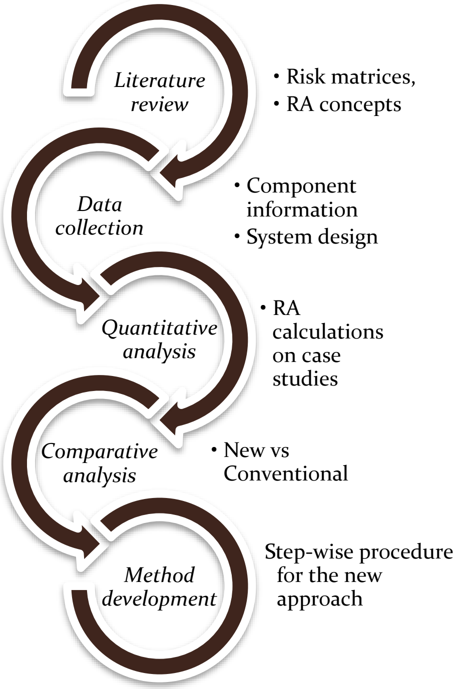

Figure 2 Methodology outline

Phase 1 (a): Initially a desk-research is to be held to understand the concepts of FMECA technique and application of RM. The FMECA process can be familiarised using the ISO31010 standards for Risk assessment techniques. However, a major study in this phase, is to analyse the current state of art for RM. A specific selection of research articles from standard journals are identified for this study. From this scientific review on literatures, the different limitations and errors of RM identified by researchers can be investigated. To explore ways to reduce these errors, a part of this study focusses upon identifying existing improvements researched by various authors. Based on the available design approaches, the most suitable type of RM to analyse infrastructure components are identified and applied. From this study the first sub-research question framed can be fulfilled.

Sub-question 1) Which risk matrix design suits best for analysing criticalities of infrastructures?

Phase 1 (b): Following this, a technical study on the concepts involved in performing RA calculations for repairable systems is made. Being the most time-consuming phase of the research sufficient period of time is scheduled for this phase. On understanding the various concepts and applications, a standardized procedure for performing repairable system calculations is used. The IEC61708:2016 standards for Reliability block diagrams were used to obtain the required formulas and procedure. To get the picture of its practical implementation, the concepts explored were applied on basic examples. From this phase of study, it was possible to sketch down a valid methodology to perform a standard RA analysis for repairable systems. As a result, answering the second sub-research question.

Sub-question 2) What is the procedure to perform RA calculations for repairable systems based on standardized IEC 61708 norms?

Phase 2: Following the desk-research, data collection on real-time projects were done with the committee's help. The data collected must comprise information on the infrastructure's design providing its internal build using different components and subsystems. Basic data such as failure frequency or $MTBF$ and MDT or mean time to repair $(MTTR)$ for each component is collected. As the scope deals with infrastructure systems. Two case studies were compiled; (a) a navigation lock system in the Netherlands and (b) a wastewater treatment plant.

Phase 3: Upon collecting the required data, we now move onto the phase of quantitative analysis. This involves the use of RA calculations procedure obtained from the previous phase. Each system calculation consists of different quantitative indicators depicting the behaviour of a system and its composite components. Two major aspects involved in this phase of research as given below,

(i) A study on the different quantitative indicators obtained from the RA calculations. This study focuses on understanding the kind of information provided by each of these indicators in the system.

(ii) Based on their contribution to provide information on a component's position and importance. The best method to incorporate these identified indicators in the conventional criticality assessment was studied.

The insights obtained from this phase provides the required information for answering the third and fourth sub-research question framed.

Sub-question 3) How can interdependencies and importance's of each component within a system be determined?

Sub-question 4) What is the best possible incorporation of calculated quantitative indicators from RA calculations in the criticality assessment of an FMECA?

Phase 4: The next phase entails the amalgamation of the various insights obtained from the previous phases. With the answers obtained, a procedure that can aid in improving the criticality assessment is laid-down. This procedure helps in eradicating the problems identified in the conventional approach. The major issues that are attempted to be solved using the new approach are (i) RM should assess components, based on their compliance to the system's performance requirements, (ii) Quantitative indicators are incorporated in the risk matrices to obtain a much accurate risk values of components and (iii) The priority of risk values for components are based on their position and importance in the system.

Sub-question 5) How can the risk matrix designed from a systems' perspective provide criticalities of components and subsystems?

Phase 5: The final phase attempts to validate the developed approach. In this phase, the developed approach is applied to the two case studies compiled during the data collection. The case studies involve an application of conventional approach to obtain a comparative analysis on the results obtained. Following this, a simplified procedure to implement the new approach is laid down. Hence on being able to answer the defined sub-questions, and with the procedure laid down in this phase it is now possible to fulfil the main-research question.

"What is an optimal approach for criticality assessment in FMECA technique to determine the ideal criticalities of repairable components present in an infrastructure system?"

SUB-CONCLUSION

The current research attempts in developing a novel approach to extend the existing conventional risk assessment approach to assess criticalities of components in an infrastructure. The research design initially provides the scope of research and the different objectives of the study. Based on the objective and the results from the problem analysis different sub-research questions were framed and a main research question was derived as well. To ensure that the objectives and goals of study are achieved, this chapter designs a meticulous research methodology with an underlying pragmatic approach to provide a well-directed approach to solve the problem. The various works involved in each phase of the research is explained in detail. The next chapter endeavours in achieving results for these questions and is given in the form of a research paper.

Chapter 4. Research article

The works and findings involved in each phase of the thesis as explained in section 3.5 of the previous chapter is provided in the form of a standalone research paper. Following a short introduction on the technical content of the research in chapter 1. The chapter 2 provides a detailed literature review on the state of art for risk matrices showcasing previous researches on its limitations and developments. Chapter 3 develops a new approach using quantitative data derived from a range of standardized reliability and availability calculations. The 4th chapter describes the implementation of the new approach on a navigation lock system (case study) along with the conventional method. The results obtained from the new and conventional methods are compared and discussed in the following chapter 5. Appendix A consists of the conventional risk matrix used for the case study. Appendix B provides the MATLAB code used for design and plotting of risk in the risk matrix used for the developed method. Finally, appendix C and D depicts the criticality assessment of components in the system using developed and conventional method.

The research paper provided in this chapter is aimed for publishing in the coming months. This research paper was iterated several times and the version number of this research paper is provided. Although a different version of the paper might be submitted to journals based on several iterations and changes according to the journal would be made before submitting, the content of this paper would remain the same. Hence a different version of the paper with the same content can be seen in future.

IMPROVED RISK ASSESSMENT FOR REPAIRABLE INFRASTRUCTURE COMPONENTS IN FMECA

R.T. Ganesh, M. Van Den Boomen, J. Hoving, A.R.M. Wolfert

Delft University of Technology, The Netherlands, Faculty of Civil Engineering and Geosciences

[Version nr.1, dated:10-04-2019]

ABSTRACT

With the number of infrastructures increasing each year, the requirement for its effective maintenance has become elemental. A Failure Mode Effect and Criticality Analysis (FMECA) is a commonly adopted technique for identifying and prioritizing critical components to develop effective maintenance plans. Risk matrices (RM) are used as a tool for criticality or risk assessment of components based on their failure probability and impacts on the system. A fundamental limitation in an FMECA is its lack of using quantitative inferences that considers a component's position and importance, to assess its risk in a system it exists. To overcome this, different RM are designed for distinct levels of a system's functional loss upon component failure and combined. Still, FMECA being a qualitative method does not explicitly account for component interdependencies such as redundancy or its failure contribution to the system's failure. This limitation results in defective maintenance planning causing unforeseen downtimes. This current research enhances the conventional risk assessment in an FMECA with a novel approach developed using unique factors obtained from reliability and availability (RA) system calculations of repairable systems. The developed method is applied to a case study along with the conventional method for a comparative analysis, from which it was evident that the new approach provides better quantitative reasonings for criticalities obtained for each component. On analyzing it was seen that, 47% percent of components were wrongly assessed as non-critical in the conventional method. This novel extension to a conventional FMECA will yield better-prioritized maintenance planning.

Keywords *– FMECA, Risk matrix, Risk assessment, Criticality assessment, Maintenance optimization*

1. INTRODUCTION

The goal of maintenance for any infrastructure is to obtain its maximum utility. Being one of the major areas of concern in the field of infrastructure management a wide-range of preventive or predictive maintenance strategies are being developed to foresee and prevent failures. But even under the best strategies, components still fail to cause corrective actions to be taken (Moubray, 1997). The direct impact for an asset owner when a component fails is the downtime incurred during its repair period. Upon failure, a component is typically repaired and brought back either to a good as new condition or a minimal repair is made to bring it back to the previous working condition (Ebeling, 2005). The current research accounts for the repairability of components under a certain maintenance strategy.

In general, any infrastructure can be considered as a system comprising several repairable or replaceable components. On visualizing them as systems, the different failure combinations that can occur based on the component's set-up and their respective impacts on the system can be identified. The most standardized technique to analyze failures and effects of each component present within a system is the FMECA method (Kapadia & Tabibzadeh, 2017). In the field of infrastructure management, FMECA's are widely used for the purpose of developing maintenance plans. Since infrastructures usually consist of several components, their maintenance actions should be prioritized based on their importance in the system. FMECA analyzes the risk of each component in the system using Risk Matrices (RM). Based on the interference between (a measure for) failure probability and impact of a component's failure, the different maintenance strategies developed are prioritized (IEC/ISO 31010:2009). The current research takes a fundamental RM as a point of departure. In such RM the probability of failure is approximated with the average failure frequency of repairable component and expressed as the reciprocal of its mean time between failure ($MTBF$). The impact of a failure is expressed as mean down time (MDT) of a failure. Naturally, RM can be extended with other impact criteria. This, however, does not alter the objective of the current research.

A fundamental limitation of an FMECA lies in the way RM are applied to analyze component criticalities. The limitation here is that RM neglects the *unique position* that certain components hold in a system. This position can be defined based on the type of configuration, a number of similar components and conditional failure rate. But in general, RM prioritizes components only based on their $MTBF$ and MDT neglecting the aforementioned uniqueness.

This occurs since, in FMECA, each component is assessed individually based on its different possible failure modes and effects (IEC/ISO 31010:2009). But the same cannot be done while analyzing criticalities of multiple similar components together or subsystems having components in a particular configuration. Because such components or subsystems hold a unique position in the system. For example, an individual component can be assessed as non-critical whereas the assessment of all similar components together as a subsystem could be assessed as critical. This problem occurs since RM are usually designed from the perspective of a system, although they are applied to and assess only individual components present in it. At times in the conventional method, different RM for distinct levels of functional loss are designed and added to a single risk matrix. Even on doing so, we still have the problem of qualitatively estimating the system's functional loss for a component failure. Also, setting consistent acceptability limits for each level of functional loss is difficult.

Due to the problems in the conventional method, erroneous results are obtained for components that are non-individual and non-independent making the developed maintenance plans less reliable. These errors sometimes cause overestimation of failures resulting in excess maintenance investments for asset owners and also vice-versa where critical components are ignored causing unforeseen system failures. This problem can be reduced by the inclusion of quantitative indicators accounting for the position held and the importance of a component in a system. The objective of the current research is to develop a quantitative method that enhances the accuracy of the conventional risk assessment in an FMECA using a RM designed based on system-specific limits. Using quantitative information would also reduce the presence of human biases in maintenance plans (Memarzadeh & Pozzi, 2016b).

The outline of the paper is as follows. Section 2 reviews the current state of art on RM presenting an analysis of its limitations and the various approaches developed by researchers to reduce them. Based on the available methods, the most suitable type of risk matrix is identified and its design using system-specific limits for analyzing components is explained. Hereafter, section 3 develops an improved method for risk assessment of repairable components in a system. Section 4 demonstrates the developed method on an infrastructure system in the Netherlands and presents a comparative analysis with the conventional method. Discussion and recommendations are presented in section 5 followed by conclusions in section 6.

2. LITERATURE REVIEW ON RISK MATRICES

Risk matrices (RM) are a tool that combines the failure frequency and impact encountered upon an event's occurrence through means of qualitative or quantitative inputs producing a risk level (IEC/ISO 31010:2009). RM work on a basic principle that, risks are the joint probability of an event occurring and its impact on the subject entity. RM, in general, have an industry-wide application in various fields to assess criticalities of risks present in projects, processes, corporate decisions, etc. Simplicity in design, its transparency, and practical applicability are the reasons for its popularity.

RM act as a means of amalgamating available qualitative or quantitative data of events to analyze their criticalities and prioritize their mitigation measures accordingly. In the field of infrastructure management, RM play a vital role in assessing the criticalities of components within systems in order to develop optimal maintenance strategies (Antosz, Stadnicka, & Ratnayake, 2017).

Although RM are widely popular they are known to have deficiencies in applications. Inferences obtained from RM can vary due to differences in perspectives and subjectivity in fixing acceptability levels. RM provide statistical information about the true but unknown quantitative risk, making them have deficient information with which accurate decisions cannot be made (Anthony (Tony)Cox, 2008). Poorly designed RM make the process of risk ranking and estimations ill-suited for decision making (Baybutt, 2015). RM are usually designed in three ways, namely, (i) Qualitative – inputs are descriptive (e.g. high, medium, low) (ii) Quantitative – input is numerical and definite (e.g.1-5). and (iii) Hybrid or Semi-Quantitative – a combination of descriptive and numerical inputs are used to define a risk (Elmontsri, 2014). Therefore, these designs are based on the type of inputs used for obtaining inferences.

Quantitative matrices are highly recommended when the required data is available (Bahill & Smith, 2009). This is because, with quantitative data, the possibility of biases in the information gathered is minimal. In the absence of such data, qualitative & semi-quantitative RM are used based on information derived from relevant literature sources and personal experiences (Pickering & Cowley, 2010). Qualitative inputs are very subjective comprising various cognitive biases and individual variability in verbal descriptions causing contrasting judgments on risks from its actual value (Peace, 2017). But this is not the case with quantitative inputs obtained from logical and reliable processes or calculations executed using real-time data. Thus, using quantitative data in RM are one of the better ways of eradicating subjective biases (Duijm, 2015).

Other major issues are associated with the errors in RM design. This occurs in both quantitative and qualitative types. A drawback that might be incurred in quantitative RM are their lack of conformity in exact estimates due to the range of values being assigned to each cell (Pickering & Cowley, 2010). Whereas, in qualitative matrices, quantifying risks based on textual inputs make their evaluation and prioritization difficult. For instance, what could be the risk value for an event having a high impact and medium probability? In such cases, incorrect risk ratings are obtained for events that might pose more serious impacts in reality. This makes the results obtained less-reliable (Elmontsri, 2014).

The most effective design for RM cannot be narrowed down to a single method since the application of RM is very subjective to their purpose of being implemented. Conventional RM are very simple to design, but these matrices have many errors and defects as described in the previous paragraphs. Apart from the above-mentioned problems, the credibility of RM is also affected due to improper scaling of axes, lack of accuracy in rating and prioritization methods. In order to improve the accuracy of RM by eliminating issues of biases and design errors, the works of literature propose two major improvement approaches namely Cox's three axioms and Iso-risk contour method.

The three axioms proposed by Cox are (i) weak consistency – the lowest risk in a red cell must be quantitatively larger than the highest risk in the green cell, (ii) betweenness – having an intermediate risk (yellow) between red and green will reduce risk reversal errors causing extreme change in results due to small increase in inputs and (iii) consistent coloring – acceptable risks should fall only on points of equal and less than the constant maximum green risk, similarly for each levels (Anthony (Tony)Cox, 2008). Cox's RM approach is based on the principle that, on eliminating possible causes of deficiencies and logical implications, a reasonable risk matrix can be designed.

The Iso-risk contour method plots and prioritizes risks using hyperbolic iso-risk lines passing through points of constant risk values (Bao, Wu, Wan, Li, & Chen, 2017). An important deficiency in RM is the risk reversal errors that occur due to the multiplication operator (probability x impact) producing lines of equal risks which a matrix cannot model accurately (Pickering & Cowley, 2010). Risk reversal errors are also caused due to the presence of several points within each cell. This can be eliminated by using the iso-risk method of design (Baybutt, 2015). The constant risk (R_0) value is determined based on acceptability levels of each category (low, medium, high). For example, when a maximum impact of 8 hours each year above which all components are considered critical, then $R_0 = 8$. Similarly, different levels (medium, low) are incorporated using their respective R_0. Thereof, contour lines for each level are obtained using Equation 1.

$$C = \frac{R_0}{L}, (1)$$

where C = consequence; R_0 = constant risk and L = likelihood.

Another important factor to be considered during design are the scales being used. Each scale has its own kind of influence on the accuracy of risk assessment. Since we favor the use of the Iso-risk method, logarithmic scales are preferred since they complement this type of RM design. Because while using a common-log scale the contour formula becomes more like a straight-line equation with a definite slope as shown in Equation 2:

$$Log(C) = R_0 - Log(L) \quad (2)$$

Differentiating risks using straight lines are much simpler than hyperbolic lines produced by linear scales (Levine, 2012). In risk assessments, events having a zero-risk value that is produced in linear scales (0-5) is of no use. Logarithmic scales overcome these issues since they do not accommodate zero events in their ranges. In addition, minimum and maximum risk levels of each cell can be determined which increases the accuracy in manual plotting (Novozhilov, 2015).

In conclusion, the current research uses a quantitative risk matrix design using the Iso-risk contour method in such a way it satisfies the three axioms of Cox's theorem. As we know, risk acceptation levels define the acceptable risk of a component. The problem faced in RM while assessing components from a system's perspective can be eliminated by the inclusion of system-specific limits. RM designed in the current research defines acceptability levels based on system performance requirements.

Logarithmic scales are used for the axes which complement the assessment of infrastructure components having failure rates of higher orders (e.g. once in 10 years, once in 25 years). To facilitate accurate plotting in log scales, a MATLAB code is provided in Appendix C. The RM designed for the current research is shown in figure 1, where x-axis represents the failure rate (or) probability of failure of repairable components (e.g. expressed as failure rate 10^2 - 1/100th per year or as $1/MTBF$: 10^{-2} - 100 years) and the y-axis represents the impact of a component's failure in MDT (hours).

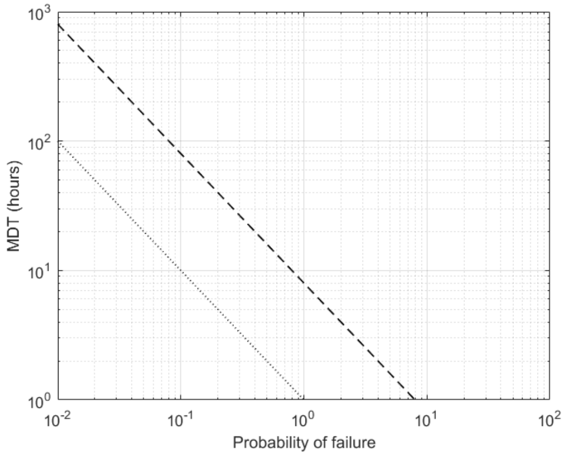

Figure 3. Illustrative RM design

In the following section, a method is developed to obtain accurate risk assessment from figure 1. This method includes the importance of a component in a system it is a part of.

3. METHOD DEVELOPMENT FOR IMPROVED CRITICALITY ASSESSMENT

Infrastructures are built up of several individual components and subsystems. These subsystems are present in various configurations within the system. A system's uptime, (i.e. operational or running time), is based on the reliability and availability (RA) of each component present in it. A component's RA depends on its actual failure rate by design and the time required for repair in order to bring it back to an upstate (Ebeling, 2005). Typically, components with lower failure rates and faster repair times contribute less to system failure and system downtime.

The system RA also depends on the configuration of these components, I.e. components in a parallel configuration will generally contribute less to a system's failure and downtime compared to components in a serial configuration. In general, we could say that components in parallel configurations are less important (critical) than components in serial configurations.

Therefore, to assess criticalities of such repairable components or subsystems we require quantitative indicators that account for their (i) repairability, (ii) design failure rate (for individual components) or conditional failure rate (for dependent components) and (iii) importance in the system. This exactly is what that has been neglected in conventional risk assessments, which only considers the components' (i) repairability and (ii) design failure rate. This section develops an improved method for inclusion of the conditional failure rate and importance in a system using quantitative indicators derived from a set of system RA calculations assuming all components in the system are repaired upon failure.

3.1 System Availability and Reliability Calculations

Reliability by definition is the probability that a component will have no failures for a given time, whereas availability is the probability that a component is operational at a certain time (Birolini, 2013; Topuz, 2009). Normally, non-repairable components upon failure are discarded. But when they are repairable, a failed component is put back into the system once its repair is done (Buzacott, 1967). And so, due to the involvement of repair times, repairable systems are not threatened as non-repairable systems.

To determine the different quantitative indicators required for each component within the system, the current research builds on approaches provided in IEC 61708:2016. Since a repairable system's failure is different due to the reasons mentioned earlier, initially an availability calculation is made, and the results obtained are then transformed into reliability characteristics. The RA calculations are supported with reliability block diagrams (RBD) which schematize a system and visualize its component relationships. An RDB depicts the way a system is built by its constituent components or subsystems having different serial and redundant configurations. Once the RBDs are constructed, the time-variant availability of each individual component ($A_c(t)$) is computed under the assumption of an underlying exponential distribution conform Equation 3.

$$A_{c_i}(t) = \frac{\mu_{c_i}}{\lambda_{c_i}+\mu_{c_i}} + \frac{\lambda_{c_i}}{\lambda_{c_i}+\mu_{c_i}} EXP\left(-\left(\lambda_{c_i}+\mu_{c_i}\right)t\right), \quad (3)$$

where μ_{c_i} = component's i repair rate, λ_{c_i} = component's i failure rate and t = time.
The component's repair rate is the reciprocal of its MDT and the failure rate is the reciprocal of its $MTBF$.

The system's availability $A_s(t)$ is computed based on availabilities of individual components using the reliable path method (e.g. Sylvester Poincaré formula as in Equation 4) or its inverse, the minimal cut sets approach (Dhillon, 2007). Using the RBD, reliable paths are identified and the system is reliable if one (or more) of its reliable paths are operational (IEC 61708:2016). Based on the identified reliable path sets the system availability equation is constructed as:

$$A_s(t) = \sum_{i\le n} A_{c_i}(t) - \sum_{i<j\le n} A_{c_i}(t)\cdot A_{c_j}(t) + \sum_{i<j<k\le n} A_{c_i}(t)\cdot A_{c_j}(t)\cdot A_{c_k}(t) - etc. \quad (4)$$

Once the components and system availabilities at each time are calculated, a so-called Birnbaum Importance Factor BIF of each component is computed according to Equation 5. A component's BIF_{c_i} is a measure for its relative importance or its contribution to the system's availability at each time. BIF displays the sensitivity of a system to become unavailable pertaining to a change in the component's availability.

$$BIF_{c_i}(t) = A_{s|c_i}(t) - A_{s|\bar{c}_i}(t), \quad (5)$$

where $A_{s|ci}(t)$ = system availability given component's C_i availability is 1 (working) and $A_{s|\overline{ci}}(t) =$ system availability given component's C_i availability is 0 (not working).

The $BIFs$ are calculated based on the difference between the conditional availability of the system given that a particular component works or loses its function. This measure can be used in quantifying the change in the system's availability due to a small change in the component's availability (Bao et al., 2017). $BIFs$ have value in prioritizing preventive and corrective actions when there are many components present within a system.

Following the BIF calculations, we can now derive the unconditional failure intensities w_{c_i} of each component. The $w_{c_i}(t)$ is a statistical mean of the intensity process at time t and is typically applied in reliability calculations during a design phase (Hokstad, 1997). Since no information is available at this time about the component's actual failure or its required maintenance, all predictions are entirely based on the information available at time 0. Hence at any instant, the predicted failure intensity for a component is equal to its $w_{c_i}(t)$. This provides the instantaneous failure rate of a component i given it was working at time zero, whereas the conditional failure intensity $\lambda_{c_i}(t)$ provides the instantaneous failure rate of a component given it was working at any time between 0 and t, assuming the component not failed at t. $w_{c_i}(t)$ can be obtained by a simple multiplication of the component's $A_{c_i}(t)$ and its respective instantaneous failure rates λ_{c_i}.

$$w_{c_i}(t) = \lambda_{c_i}(t) \cdot A_{c_i}(t) \text{ (6)}$$

This unconditional failure intensity is also known as rate of occurrence of failures ($ROCOF$), whereas the conditional failure intensity $\lambda_{c_i}(t)$ is also known as hazard rate. Consequently, to obtain the system's unconditional failure rate $w_s(t)$ or $ROCOF_s$, we use the obtained BIF_{c_i} (Equation 5) and w_{c_i} (Equation 6) of each component present in the system conform Equation 7. This gives us an equivalence of the total unconditional failure intensity of a system at any time between 0 to t.

$$w_s(t) = \sum_i BIF_{c_i}(t) \cdot w_{c_i}(t) \text{ (7)}$$

However, a measure of interest for the application in RM is not the expected number of failures at a certain time $w_s(t)$, but instead the time for first (or next) system failure to occur or the mean time between system failures ($MTBF_S$). Ultimately, the interest lies in obtaining the conditional failure intensity of a system for its application in RM. To obtain this indicator, we move on to estimating the conditional failure intensity $\lambda_{vs}(t)$, also known as the Vesley failure rates or hazard rates derived from the $w_s(t)$ and $A_s(t)$. An underlying assumption is that when a component fails, the system stays in a steady state. At this steady state, the conditional failure intensity provides a useful approximation of the system's failure rate. To determine this, we require a transform from unconditional system failure intensity to conditional system failure intensity as defined in Equation 8. When the conditional failure rate of a system reaches an asymptotic value, this transform follows a similar relationship as in Equation 6, but at the system level (IEC 61708:2016).

$$\lambda_{vs}(t) = \frac{w_s(t)}{A_s(t)} \text{ (8)}$$

The $\lambda_{vs}(t)$ obtained is either constant or asymptotic based on the configuration in which the system is built.

The average of constant conditional failure intensity $\lambda_{vs}(t)$, gives the constant failure rate ($\lambda_{avg,vs}$), and for an asymptotic distribution, an average value can be approximated to its asymptotic value ($\lambda_{asy,vs}$) conform to the relationship, $\lambda_{avg,vs} \sim \lambda_{asy,vs}$ (IEC 61708:2016) . This average $\lambda_{avg,vs}$ (constant rate) can be used for the conventional reliability calculations well-known for non-repairable systems (time to first failure or time from one failure to the next failure). The reliability of the system provides a measure of how the system behaves with respect to time. The time-variant system reliability (to the first failure) at each instance between 0 and t can be calculated using the average Vesely failure rate ($\lambda_{avg,vs}$) as given in Equation 9.

$$R_s(t) = EXP\left(-\lambda_{avg,vs} \cdot t\right) \text{ (9)}$$

The measure of interest for RM as explained earlier i.e. system $MTBF_S$ is determined as $\frac{1}{\lambda_{avg,vs}}$. Another interesting measure of any system's availability calculation is its mean downtime (MDT). The MDT of a system (or $\frac{1}{\mu_s}$) is derived using the $A_s(t)$ and $\lambda_{avg,vs}$. This is done by solving Equation 3 in two ways, (i) isolating μ_s for the known $A_s(t)$ and $\lambda_{avg,vs}$ and using the Taylor's expansion for the non-linear part of the equation as shown in Equation 10 or (ii) using a trial and error method for μ_s at each time.

$$A_s(t) = \frac{\mu_s}{\lambda_{avg,vs}+\mu_s} + \frac{\lambda_{avg,vs}}{\lambda_{avg,vs}+\mu_s}\{\lambda_{avg,vs}(1-(\lambda_{avg,vs}+\mu_s)t+\cdots)\} \quad (10)$$

3.2 Indicators for criticality assessment

A criticality assessment is generally applied on the component level. Section 3.1 provides the procedure to calculate the quantitative indicators of repairable components based on an RA system calculation. The system indicators provide the required information to assess system compliance. To assess a component within the system properly, we need the indicators $MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$, MDT_{c_i} and BIF_{c_i}.

However, a conventional risk assessment uses only the $MTBF_{c_i}$ as an estimate for a component's time to failure and MDT_{c_i} as an impact measure (downtime) for its failure. Risk follows from their inference in a conventional FMECA where we analyze each component individually ($Risk = MTBF_{c_i} * MDT_{c_i}$). We therefore propose an extended measure which includes its relative importance in a risk assessment.

First, the BIF needs an additional transform. The BIF_{c_i} are a typical importance measure at a component level (Purba & Deswandri, 2018). This increases our interest in incorporating this measure in conventional FMECA. BIF_{c_i} are calculated as explained in 3.2, it measures the sensitivity of a system to fail when a change is made in its component. So, when a very high BIF_{c_i} is seen, usually additional redundancy is provided to those components. However, the main disadvantage of using BIF as an indicator is its negligence of considering the probability of failure events. When two basic events play similar roles their ranking according to the Birnbaum Importance Measure becomes extremely close (or identical) although their probabilities may differ in great orders. Hence, no matter how attractive its physical interpretation of sensitivity analysis is, BIF_{c_i} are only used as a reference value (Dutuit & Rauzy, 2015).

To overcome this dilemma, we propose the inclusion of Lambert's importance measure or otherwise known as the criticality importance factor (CIF) Since we are interested in identifying the component that has the highest probability to cause system failure, $CIFs$ are the most useful importance measure. It can be defined as the conditional probability that a component is critical in a system and fails at t, given the system fails at the same time (Chybowski & Gawdzińska, 2016).

To find the criticality importance of a component i, (CIF_{c_i}) in a system following Lambert's importance measure, we link the BIF_{c_i} and unavailability of a component and the system's unavailability (IEC 61708:2016) conform to Equation 11. The system unavailability ($1 - A_s(t)$)

follows from Equation 4, is at each time the same for all basic events, and has no influence while ranking components in a system (Dutuit & Rauzy, 2015). Thus, overcoming the problem of obtaining very close values as experienced while using $BIFs$.

$$CIF_{c_i}(t) = BIF_{c_i}(t) * \frac{1-A_{c_i}(t)}{1-A_s(t)} \quad (11)$$

$CIFs$ are moreover a normalized $BIFs$ which also accounts for the individual components' unavailabilites. $CIFs$ provide the percentage contribution of a component to the system's failure at each time from 0 to t, making them rank components based on less closer values. In maintenance planning, this measure provides us advice on which component to be repaired first to reduce a fraction of its risk in the system (Vaurio, 2016). With their inclusion in RM, we can not only compute risk values but also prioritize components based on their importance to the system. Since $CIFs$ can be calculated for all independent components and sub-systems, we can prioritize maintenance actions of components within each subsystem based on the importance of latter in the system as well.

3.3 Incorporating quantitative data in risk assessment

On obtaining all components and system metrics from the previous steps, we can now assess whether the system complies with the risk acceptation levels or performance requirements. The system can be assessed for compliance based on the metrics A_s, $MTBF_S$ and MDT_S obtained from section 3.1. If the system complies to the requirements during the first RA assessment, we can establish maintenance strategies. The interventions are prioritized based on risk values obtained from Equation 12. Compliant level of maintenance should be implemented for each component i.e. higher risk values will have stricter maintenance requirements and vice versa. Maintenance intervals will be based on the component's $MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$, with a fitting confidence interval, in such a way that they have early maintenance actions planned.

If the system does not comply, we need to improve the components present in it either by maintenance or design. We can understand the component's condition from the computed metrics such as $MTBF_{c_i}$, MDT_{c_i}, A_{c_i}, BIF_{c_i} and CIF_{c_i}. A component's $MTBF_{c_i}$ and MDT_{c_i} can be improved either by adding redundancy or making changes in its fundamental design. The $CIFs$ provide information on the critical components to be improved first. Following enhancement, a new RA system calculation will demonstrate whether the system complies with the risk acceptation levels. If it does, maintenance strategies can now be established, using $MTBF_{c_i}$ for intervention intervals (with proper confidence intervals) and $Risk_{c_i}$ for prioritizing.

To obtain $Risk_{c_i}$values for prioritization, the developed method proposes the incorporation of CIF_{c_i} and MDT_{c_i} of each component. CIF_{c_i} provides the likelihood of failure for components critical to system failure, given that the system has also failed at the same time. In other words, the probability that a component will become critical for system failure and actually fails. Hence, CIF_{c_i} gives us the probability that a component causes system failure and MDT is the impact incurred upon the event's occurrence. On incorporating CIF in RM we propose to assess the risk priority of each component quantitatively based on its importance conform Equation 12.

To obtain $Risk_{c_i}$ values for prioritization, the developed method proposes the incorporation of

$$Risk_{c_i} = CIF_{c_i} * MDT_{c_i} \text{ (12)}$$

Where $Risk_{c_i}$ is the risk value of a component i, CIF_{c_i} is the criticality importance obtained for component i from time 0 to t and MDT_{c_i} is the mean down time of component i.

In conclusion, the current research extends the conventional risk assessment based on quantitative data derived from the system's RA calculation. An added value achieved in the design of a single RM is its continuous risk assessment and prioritization using acceptation levels derived from SLA which would be demonstrated in the following case study.

4. CASE STUDY – A COMPARATIVE ANALYSIS

As an illustrative case study, a navigation lock system in the Netherlands is used whose primary function is to protect land against high tidal water while allowing for ship passing. The conventional risk matrix for the lock system is presented in Appendix A. In the case study a novel quantitative RM is designed with risk acceptation levels based on system performance requirements. Hereafter, a system RA calculation demonstrates whether the system complies to the performance requirements. Moreover, the system RA calculation provides metrics for the importance of components in the system configuration and allows for their risk assessment.

The lock system is constructed in parallel as shown in Figure 2. At least one of the two locks must have an upstate at any given time for the system to fulfill its function. The system is decomposed based on a typical lock design (A.Glerum & A.Vrijburcht, 2000) as depicted in Figures 3 and 4. The system is simplified for a better interpretation of the developed method. Table 1 provides basic information on each individual component (λ_{c_i}, MDT_{c_i}) present in the system.

According to the performance requirements or service level agreements (SLA) specified by the asset owner, the lock must have an availability of 99.8% each year including its planned downtime. The remaining 0.2% accounts for the unplanned (or) accidental downtimes incurred upon unforeseen failures. Since components fail no matter how accurate the interventions are, strategies must be developed such that the unforeseen failures conform within the tolerable limit (0.2% or 18 hours per year).

The RM is designed using the Iso-risk method identified from the literature study. To include system requirements in the RM, acceptability levels are defined based on the permissible unplanned downtime set out in the SLA. With a maximum 0.2% of unplanned downtime, 18 hours each year, system criticality complies to $Risk_{ci} \geq 18$ (dashed line). For the case study components with a

$Risk_{ci} \leq 1$ and $R_0 = 1$ are non-critical (dotted line). The portion lying amid these lines is the intermediate risk zone. The RM designed for the case study is as shown in figure 5.

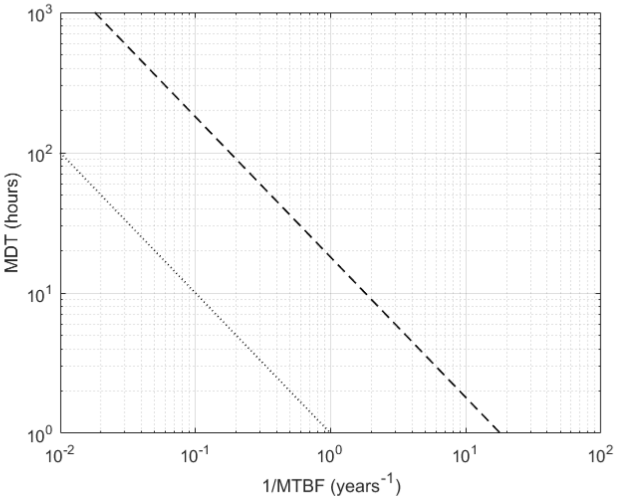

Figure 4. RM for the case study

Next, the different component and system metrics that provide the required quantitative information to check the system's compliance are calculated. This case study follows the procedure of RA calculations as explained in 3.1, following a steady state approach for demonstration purposes. The steady-state availabilities of components are shown in Table 1.

Table 2. Basic component data

Components	λ_{c_i}	$MTBF_{c_i}$	MDT_{c_i}
	(hours-1)	($1/\lambda_{c_i}$) (years)	(hours)
Drive installation	5.71E-06	20.0	16
Levelling gate	1.90E-05	6.0	48
Rolling carriage	9.51E-06	12.0	72
Cable	1.90E-05	6.0	4
Sleeve	4.57E-06	25.0	72
Tensioning device	4.57E-06	25.0	42
Steel door	1.40E-06	81.5	72
Wearing course	3.81E-06	30.0	96
Hardware CS	5.71E-05	2.0	24
CPU CS	4.57E-06	25.0	48
Lock head	7.61E-06	15.0	140
Operation system	5.71E-06	20.0	24
Low voltage system	2.85E-06	40.1	72
Guide pilings	3.04E-06	37.5	72
Lock chamber walls	2.85E-06	40	336
Level measurement system	7.61E-06	15.0	36

Using the failure rates (λ_{c_i}) and mean downtime of each component (MDT_{c_i}), its steady state availability (A_{c_i}) is calculated following Equation 13. The steady state system availability is calculated conform Equation 4.

$$A_{c_i} = MTBF_{c_i}/(MTBF_{c_i} + MDT_{c_i}) \quad (13)$$

Hereafter, the sensitivity of each component within a (sub)system (BIF_{c_i}) is calculated with Equation 5. Components with higher BIF values are the most sensitive to changes. The CIF_{c_i} is calculated using the components' BIF_{c_i} and unavailability $\left(1 - A_{c_i}\right)$ and system unavailability $(1 - A_s)$ conform to equation 11. From the $CIFs$ obtained we can identify components that hold a high importance in the system (i.e.) the component having a high influence on system failure. The CIF values for each component are shown in Table 2.

Table 3. Quantitative data from system RA calculation for subsystem rolling gate

Components	A_{c_i}	A_s	BIF_{c_i}	CIF_{c_i}	w_{c_i} (hours-1)
Drive installation 1	0.9999086	1.0000	9.11E-05	2.8E-06	5.71E-06
Drive installation 2	0.9999086		9.11E-05	2.8E-06	5.71E-06
Levelling gate 1	0.9990888	1.0000	0	0.00	1.90E-05
Levelling gate 2	0.9990888		0	0.00	1.90E-05
Levelling gate 3	0.9990888		0	0.00	1.90E-05
Levelling gate 4	0.9990888		0	0.00	1.90E-05
Levelling gate 5	0.9990888		0	0.00	1.90E-05
Rolling carriage 1	0.9993157	1.0000	0.0006822	1.6E-04	9.50E-06
Rolling carriage 2	0.9993157		0.0006822	1.6E-04	9.50E-06
Cable	0.9999240	0.999924	0.9970712	0.03	1.90E-05
Sleeve	0.9996711	0.999671	0.9973235	0.11	4.57E-06
Tensioning device 1	0.9998081	0.9992326	0.9971868	0.06	4.57E-06
Tensioning device 2	0.9998081		0.9971868	0.06	4.57E-06
Tensioning device 3	0.9998081		0.9971868	0.06	4.57E-06
Tensioning device 4	0.9998081		0.9971868	0.06	4.57E-06
Steel door	0.9998992	0.9998992	0.9970959	0.03	1.40E-06
Wearing course	0.9996344	0.9996344	0.9973601	0.12	3.81E-06
Hardware CS	0.9986315	0.9986315	0.9983617	0.45	5.70E-05
	A_s	0.99699543		w_s	1.039E-04
	λ_{vs} (hours^{-1})	$MTBF_s$ (years)	MDT_s (hours)		
Subsystem rolling gate	0.000104174	1.10 (years)	28.93 (hours)		

To assess system compliance the system's $MTBF$ and system's MDT need to be calculated as explained in section 3.1. This procedure is demonstrated for the subsystem rolling gates. First, the rate of occurrence of failures ($ROCOF_{c_i}$ or w_{c_i}) for each component follows from Equation 6. Hereafter, Equation 7 provides the unconditional failure intensity of the system (w_s). The conditional failure rate or Vesley failure rate (λ_{vs}) needs the w_s and the system's A_s as input and follows from Equation 8. The $MTBF_s$ of the system is obtained from $\frac{1}{\lambda_{vs}}$. Finally, the MDT_s is calculated by solving the steady state availability equation as shown in Equation 14.

$$MDT_s = MTBF_s * \frac{(1 - A_s)}{A_s} \quad (14)$$

Following the same procedure as mentioned in the above paragraphs the RA calculation is raised to lock system. These calculations are presented in Table 3 and requires an assessment for compliance with system performance.

The system complies to the performance requirements when its probability of failure (or) $MTBF_s$ or (29.23 years) and impact (or) MDT_s (17.22 hours) are in accordance to the SLA. From the RM designed for this case study (Figure 6), it is seen that the system holds a position in the acceptable zone. Hence, the system complies with the performance requirements. If it had fallen in the critical zone or close to it (intermediate zone), improvements in design and redundancy of critical components should be done. Case in point, if improvement was required, the $CIFs$ identify that rolling gates and lock head hold the highest criticality among subsystems. To reduce the impact of rolling gate, we need to analyze which of its internal component can be improved. From the CIF_{c_i} of component within the rolling gates, hardware CS, wearing course and cable sleeve holds the highest criticality. Improvements in design or redundancies can increase their $MTBF$ and reduce its MDT.

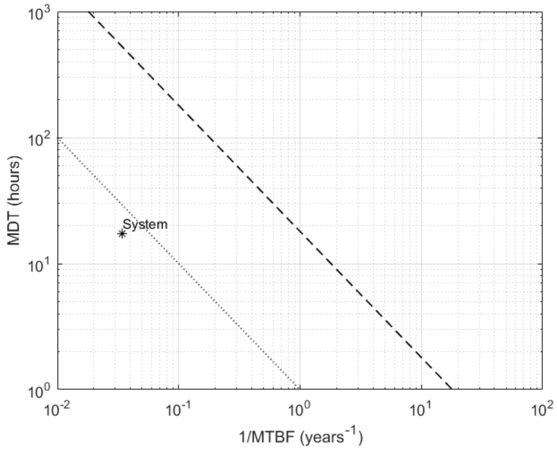

Figure 5. System compliance

Once the system complies with the SLA, well-prioritized maintenance strategies can be developed. To obtain priorities, the risk values of each component and subsystem are plotted in the RM designed as shown in Figure 4. The $Risk_{ci}$ of each component and subsystem is calculated using their respective MDT (impact) and CIF (probability of failure). Plotting in the RM was done in MATLAB using the code given in appendix B but can also be performed in Excel. The risk value of each component is presented in Appendix C. For instance, the tensioning device having a CIF_{c_i} of 0.06 and MDT_{c_i} of 42 hours is plotted in the intermediate zone. From its λ_{c_i}, the $MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$ is computed as 25 years. Maintenance interval are established based on this $MTBF_{c_i}$ and a required or preferred confidence interval. Similarly, each component is assessed, and their maintenance strategies are planned based on its $Risk_{c_i}$ and $MTBF_{c_i}$.

Table 4. Quantitative data from system RA calculation for the lock system

Components	A_{c_i}	A_s	BIF_{c_i}	CIF_{c_i}	w_{c_i} (hours-1)
subsystem rolling gate 1 (West)	0.996995	0.991799015	0.008158	0.364	1.04E-04
subsystem rolling gate 2	0.996995		0.008158	0.364	1.04E-04
subsystem lock head 1	0.999467		0.008138	0.065	3.81E-06
subsystem lock head 2	0.999467		0.008138	0.065	3.81E-06
CPU CS 1	0.999781		0.008136	0.027	4.57E-06
Operation system 1	0.999863		0.008135	0.017	5.71E-06
Low voltage system 1	0.999795		0.008135	0.025	2.85E-06
Guide pilings 1	0.999781		0.008135	0.013	1.52E-06
Guide pilings 2	0.999781		0.008135	0.013	1.52E-06
Lock chamber walls	0.999042		0.008135	0.012	2.85E-06
Level measurement system	0.999726		0.008136	0.033	7.61E-06
subsystem rolling gate 1 (East)	0.996995	0.991799015	0.008158	0.364	1.04E-04
subsystem rolling gate 2	0.996995		0.008158	0.364	1.04E-04
subsystem lock head 1	0.998936		0.008138	0.065	3.81E-06
subsystem lock head 2	0.998936		0.008138	0.065	3.81E-06
CPU CS 1	0.999781		0.008136	0.027	4.57E-06
Operation system 1	0.999863		0.008135	0.017	5.71E-06
Low voltage system 1	0.999795		0.008135	0.025	2.85E-06
Guide pilings 1	0.999781		0.008135	0.013	1.52E-06
Guide pilings 2	0.999781		0.008135	0.013	1.52E-06
Lock chamber walls	0.999042		0.008135	0.012	2.85E-06
Level measurement system	0.999726		0.008136	0.033	7.61E-06
	A_s	0.999932744		w_s	3.90E-06
	λ_{vs} (hours^{-1})	$MTBF_s$ (years)	MDT_s (hours)		
Hansweert Lock System	3.90E-06	29.23 (years)	17.22 (hours)		

For comparison, a traditional FMECA is conducted with the conventional RM as depicted in Appendix A. It is observed that this conventional risk assessment approach tries to incorporate the importance of components to a system failure by adding additional RM. Each matrix is designed for a specific range of functional loss having different acceptability levels in each of them. The risk assessment lies on qualitative judgment of the impact of component failure on system downtime. Selecting the proper RM will become more difficult when complexity of the system increases.

The traditional approach further assumes that all components and subsystems fail at their $MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$. The impact produced is equal to their MDT_{c_i}. The risk values follow the typical interference of a conventional risk assessment, $Risk = MTBF_{c_i} \cdot MDT_{c_i}$ as shown in Appendix A (RM) and Appendix D (results). The scales used in this RM are linear where each cell comprises a range of values.

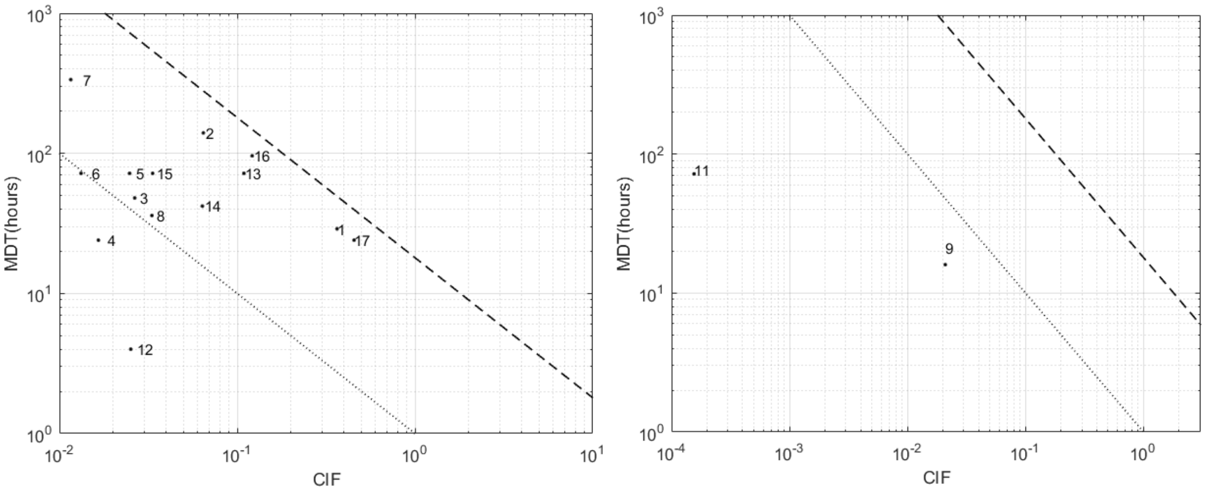

Figure 6 Components plotted in the designed RM using data from Appendix

Such RM are designed for different functional loss incurred by the system upon a component's failure. For instance, to assess the risk of tensioning devices, we know that this component has a serial configuration, and upon failure, the system loses 50% of its functionality. Now the component is plotted based on its $MTBF_{c_i}$ (25 years) and MDT_{c_i} (42 hours) in cell 8 of RM-3. We assign the risk value of the entire cell, making it non-critical. Similarly, each component's risk is assessed based its contribution to the system's functional loss, component metrics ($MTBF_{c_i}$ and MDT_{c_i}) using the conventional RM. Results of comparison between the conventional and novel approach are discussed in the next section.

5. DISCUSSIONS AND RECOMMENDATIONS

From Appendix C and D, we get an overview of the risks obtained from both methods. On a comparative analysis, differences of 47% in the values are observed. It is evident that the developed RM and method provides a better quantitative assessment since components assessed as non-critical in the conventional method were more critical in the new approach. Components were underestimated as non-critical in the conventional method but based on its importance to the system (CIF_{c_i}) it was assessed as an intermediate risk in the developed method. The lock subsystem was wrongly assessed in the conventional method due to two main reasons, (i) we neglect the configuration's behaviour and importance in the system and are assessed as individual components and (ii) presence of design errors in the RM used.

Certain individual components were also incorrectly assessed due to deficiencies in designing a RM from a system's perspective. One of the errors with this RM is that we only assign the risk value of the entire cell. Hence, components having similar risks fall in the same cell and cannot be differentiated. This is because the RM neglects the possibility of different points present within a cell having values that are quantitatively larger than others (Anthony (Tony)Cox, 2008). This type of risk assessment includes a range of qualitative assumptions while plotting risks. Qualitative assumptions involved in estimating the impact of component failure to system failure based on the categories of functional losses causes errors in the criticalities obtained. Due to the lack of quantitative reasoning and the problem of setting risk acceptation levels for each range of functional loss, incurrence of errors in results are high.

Table 5. Comparative analysis of criticalities obtained from both methods

Components and subsystems	Criticalities Obtained	
	Developed method	Conventional method
1. Subsystem rolling gate	Medium	Medium
2. Subsystem lock head	Medium	Low
3. CPU CS	Medium	Low
4. Operation system	Low	Low
5. Low voltage system	Medium	Low
6. Guide pilings	Low	Low
7. Lock chamber walls	Medium	Medium
8. Level measurement system	Medium	Low
9. Drive installation	Low	Low
10. Levelling gate	Low	Low
11. Rolling carriage	Low	Low
12. Cable	Low	Low
13. Sleeve	Medium	Low
14. Tensioning device	Medium	Low
15. Steel door	Medium	Low
16. Wearing course	Medium	Low
17. Hardware CS	Medium	Medium

▇	High
▆	Med
▒	Low

These design errors are solved in the developed method using the iso-risk RM design which eliminates the existence of risk reversal errors. A single system-specific RM is used for analyzing components based on unvarying acceptability levels. Since we design RM based on SLA of infrastructures and use RA system calculations for substantiations, it can check the system's compliance to the SLA based on components combined performance conforming to its design.

Although we are interested in observing differences in criticalities obtained from the new and conventional method. One of the major problems faced in the conventional method is the use of qualitative assumptions for prioritizing and selecting intervals of maintenance actions. These qualitative inputs lead to the existence of personal biases in the developed maintenance plans. But in the developed method, we prioritize actions quantitatively using $CIFs$ without any subjective judgements. At times, even components having a low MDT result in higher criticality due to its position and importance in the system.

Maintenance priority of each component is obtained from $Risk_{c_i} = CIF_{c_i} * MDT_{c_i}$ and the maintenance intervals are derived from its $MTBF_{c_i}$. This adds value to the existing FMECA technique because better prioritized maintenance actions can be obtained using quantitative data. Thus, the new risk assessment provides scope for achieving the current research's major objective. Given that the developed method provides a better risk assessment, care is required when acceptability levels (R_0) are set for more than one failure a year (e.g. n failures of k hours per year). Errors in setting these limits can overlook certain critical components as non-critical. Using the maximum acceptable risk for a single failure, based on the system's SLA would aid in overcoming the problem identified. This consideration provides a better baseline for experts to imply system-specific limits in RM and prioritize components in a much-reliable way.

A qualitative proposition for incorporating $CIFs$ in a conventional risk assessment is to use them as a reference index to develop better maintenance strategies. The risk of each component is calculated using the conventional interferences of $MTBF_{c_i}$ and MDT_{c_i} With the risk values, we can now prioritize components using its $CIFs$ as an index. Case in point, this method includes the manual interventions for prioritizing components. This is two-edged since, it also gives an opportunity to develop different strategies to analyze which yields better results. But due to the subjectivity of experts, variances in results are obtained. This is because attitudes of each expert and asset owner is different and this influences the strategies being used (Bevilacqua & Braglia, 2000). When such deviances are not appreciable, we recommend the use of the developed method.

6. CONCLUSION

This research develops a new method for risk assessment to overcome its limitation of not accounting a component's interdependency and importance in a system. Initially, an extensive study was made on the available RM design approaches, based on which the most suitable RM was identified and used in this research. The developed method uses a range of quantitative inputs derived from traditional repairable system's RA calculations. This method was then applied to an infrastructure case along with the conventional method to have a comparative analysis. From the results, it was clear that the new approach provides a better risk assessment since it uses quantitative indicators that account for the negligence's incurred in the conventional method. As an added value to the FMECA, the new method provides better inferences to develop effective maintenance planning. We believe that this method will be a good basis to develop new cost-effective, utility-driven and optimized maintenance strategies for any infrastructure.

APPENDIX

A. Conventional RM

Risk matrix No.	Effect Category	Frequency	Less than once per 100 years	Once per 100 years	Once per 10 years	Once per year	Once per month	Once per week
RM-1	0-20% loss of function	24 hours loss of function	░	░	░	░	░	▒
		24 hours - 1-week loss of function	░	░	░	░	▒	▓
		1 week - 1-month loss of function	░	░	░	▒	▓	▓
		1 month - 6 months loss of function	░	░	▒	▓	▓	▓
		6 months - 1-year loss of function	░	▒	▓	▓	▓	▓
		>1-year loss of function	▒	▓	▓	▓	▓	▓
RM-2	21-40% loss of function	I - < 8 hours loss of function	░	░	░	░	░	▒
		II - 8 hours - 24 hours loss of function	░	░	░	░	▒	▓
		III - 24 hours - 1-week loss of function	░	░	░	▒	▓	▓
		IV - 1 week - 1-month loss of function	░	░	▒	▓	▓	▓
		V - 1 month - 6 months loss of function	░	▒	▓	▓	▓	▓
		VI - > 6 months loss of function	▒	▓	▓	▓	▓	▓
RM-3	41-60% loss of function	I - < 2 hours loss of function	░	░	░	░	░	▒
		II - 2 hours - 8 hours loss of function	░	░	░	░	▒	▓
		III - 8 hours - 24 hours loss of function	░	░	░	▒	▓	▓
		IV - 24 hours - 1-week loss of function	░	░	▒	▓	▓	▓
		V - 1 week - 1-month loss of function	░	▒	▓	▓	▓	▓
		VI - > 1-month loss of function	▒	▓	▓	▓	▓	▓
RM-4	61-80% loss of function	I - < 1-hour loss of function	░	░	░	░	░	▒
		II - 1 hour - 2 hours loss of function	░	░	░	░	▒	▓
		III - 2 hours - 8 hours loss of function	░	░	░	▒	▓	▓
		IV - 8 hours - 24 hours loss of function	░	░	▒	▓	▓	▓
		V - 24 hours - 1-week loss of function	░	▒	▓	▓	▓	▓
		VI - > 1-week loss of function	▒	▓	▓	▓	▓	▓
RM-5	81-100% loss of function	I - < 1 / 2 hours loss of function	░	░	░	░	░	▒
		II - 1 / 2 hours - 1-hour loss of function	░	░	░	░	▒	▓
		III - 1 hour - 2 hours loss of function	░	░	░	▒	▓	▓
		IV - 2 hours - 8 hours loss of function	░	░	▒	▓	▓	▓
		V - 8 hours - 24 hours loss of function	░	▒	▓	▓	▓	▓
		VI - > 24 hours loss of function	▒	▓	▓	▓	▓	▓

B. MATLAB code for RM

```
x = linspace(0.01,100,1000);
y1 = 1./x;
y2 = 18./x;
loglog(x,y1)
hold on;
loglog(x,y2)
hold on;
grid on;
A = xlsread('FMECA.xlsx','RM','A2:A20');
B = xlsread('FMECA.xlsx','RM','B2:B20');
plot(A,B,'rx','linewidth',2);
ylim([10^-1 10^3])
xlabel('Failure rate (or) MTBF (1/hr)');
ylabel('Total MDT (or) Impact (hrs)')
```

Criticality assessment using the developed RM and method

Components and subsystems	**Effect Analysis**			**Criticality (Designed RM)**
	CIF_{ci}	MDT_{ci}	$Risk_i$	
1. Subsystem rolling gate	0.230	28.93	6.65	Medium
2. Subsystem lock head	0.081	140	11.37	Medium
3. CPU CS	0.081	48	3.90	Medium
4. Operation system	0.017	24	0.40	Low
5. Low voltage system	0.010	72	0.75	Medium
6. Guide pilings	0.016	72	1.13	Low
7. Lock chamber walls	0.017	336	5.62	Medium
8. Level measurement system	0.073	36	2.63	Medium
9. Drive installation	2.09E-02	16	0.33	Low
10. Levelling gate	0.00E+00	48	0.00	Low
11. Rolling carriage	1.55E-04	72	0.01	Low
12. Cable	0.025	4	0.10	Low
13. Sleeve	0.109	72	7.86	Medium
14. Tensioning device	0.064	42	2.68	Medium
15. Steel door	0.033	72	2.41	Medium
16. Wearing course	0.121	96	11.65	Medium
17. Hardware CS	0.455	24	10.91	Medium

▨	High
▨	Med
▨	Low

D. Criticality assessment using the conventional RM and method

Components and subsystems	Effect Analysis			Criticality (Conventional RM)
	$MTBF_{c_i}$	MDT_{c_i}	$Risk_{c_i}$	
1. Subsystem rolling gate	1.11	28.93	32.03	Medium
2. Subsystem lock head	15.16	140.00	2121.80	Low
3. CPU CS	25.24	48.00	1211.45	Low
4. Operation system	20.20	24.00	484.79	Low
5. Low voltage system	40.47	72.00	2913.86	Low
6. Guide pilings	37.89	72.00	2728.03	Low
7. Lock chamber walls	40.42	336.00	13579.52	Medium
8. Level measurement system	15.16	36.00	545.63	Low
9. Drive installation	19.99	16.00	319.87	Low
10. Levelling gate	6.01	48.00	288.39	Low
11. Rolling carriage	12.00	72.00	864.27	Low
12. Cable	6.01	4.00	24.03	Low
13. Sleeve	24.98	72.00	1798.51	Low
14. Tensioning device	24.98	42.00	1049.13	Low
15. Steel door	81.54	72.00	5870.84	Low
16. Wearing course	29.96	96.00	2876.35	Low
17. Hardware CS	2.00	24.00	47.98	Medium

▨	High
▨	Med
▨	Low

SUB-CONCLUSION

The research paper provided in this chapter describes the different works involved in answering the framed research questions. From the paper we can deduce that the new approach provides a much better assessment of risks in comparison to the conventional method. Although the paper only consists of a single case study and a short discussion section the following chapters of this report provides additional illustrations on the new method, a detailed discussion and recommendations on the results are made along with a holistic conclusion of the entire research.

Chapter 5. Additional illustrations

The purpose of this chapter is to provide additional explanations to the work showcased in the previous chapter (research paper). A well-detailed methodology of the developed approach is provided for a better interpretation of the new approach. Using which an additional case-study is performed step-wise for the developed method. Also, a comparative study on results is derived for the case study using the conventional method.

5.1 SIMPLIFIED METHODOLOGY FOR IMPLEMENTATION

This section of the chapter provides a well-delineated procedure to carry out the developed approach to assess accurate risks of component and subsystems. This methodology provides a clear step-wise procedure to check if a system fulfills its intended function (performance requirements) and the process of improvements. Following the methodology meticulously the steps involved in designing a risk matrix and assessing risk levels of components and their prioritization can be obtained.

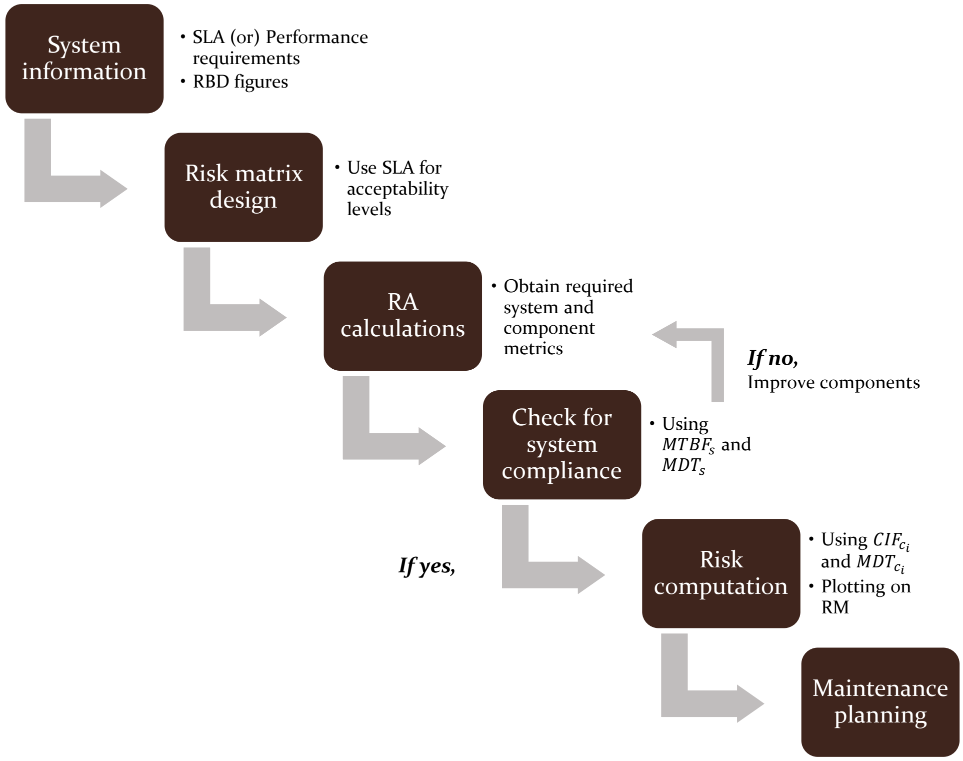
System information
• SLA (or) Performance requirements
• RBD figures
Risk matrix design
• Use SLA for acceptability levels
RA calculations
• Obtain required system and component metrics
If no,
Improve components
Check for system compliance
• Using $MTBF_s$ and MDT_s
If yes,
Risk computation
• Using CIF_{c_i} and MDT_{c_i}
• Plotting on RM
Maintenance planning

Figure 7 Simplified methodology for developed method

Step 1 → System and component information

To begin with the procedure, initially we obtain information on the asset owner specifications for the infrastructure. In this step, we obtain the various performance requirements (or) service level agreements (SLA). These requirements provide an insight into the required availability for the infrastructure each year. This gives us a baseline to determine the maximum planned and unplanned downtime that is acceptable during a year. Following this, information on the system's design and its typical component condition such as λ_{c_i}(instantaneous failure rate) and MDT_{c_i} (mean downtime) are collected for each individual component. The system's internal build can be deduced from its typical design. The system layout is represented using reliability block diagrams (RBDs') for a better visualization on the component's position.

Step 2 → Risk matrix design

Using the information of performance requirements, we can move on to designing the risk matrix for the infrastructure. Acceptability levels of a risk matrix have a major influence on the criticalities obtained. Since the current research uses iso-risk design method, the required R_0 values for the iso-risk lines are derived directly from the SLA. The unplanned downtime is the maximum permissible impact that can be incurred by the system. This gives the required constant risk value (R_0) for the critical limit (or) the minimum risk for a component, equal or above which they become critical to the system. Sufficient buffer is considered for the acceptable limit (or) maximum risk for a component to be non-critical. Following these limits, we can now design a system-specific risk matrix.

Step 3 → **Reliability and availability calculations**

The next step comprises of an extensive reliability and availability calculations using the basic component data (λ_{c_i} , MDT_{c_i}). In this step we obtain the required system and component metrics for compliance check and risk assessment. The different concepts and equations involved in the course of calculations are provided in the research paper (Chapter 4). The equations and formula provided in the previous chapter covers all the required information to carry out this step effectively. Therefore, the different system metrics namely $MTBF_s$, MDT_s and A_s and component metrics such as $MTBF_{c_i}$, MDT_{c_i}, A_c, BIF_{c_i} and CIF_{c_i} depicting its state in the system are obtained from these calculations. From the obtained metrics, we can now compute the risk values ($Risk_i$) of each component using its CIF_{c_i} and MDT_{c_i}.

Step 4 → **Check for system's compliance**

Next step checks the system's compliance to its performance requirements (or) SLA, using the system metrics ($MTBF_S$ and MDT_S). To do so, we can plot the system's $MTBF_S$ (or) ($1/\lambda_{vs}$) and MDT_S on the risk matrix. Based on the location of the system in the risk matrix, we can identify if the system complies to the SLA. The two action flows of this step are (i) If the system falls in the acceptability zone, we can move on to component assessment or, (ii) If the system falls away from the acceptability zone, the components must be improved either by design or by adding redundancy to its layout in the system. From the risk values ($Risk_i$), the components having a higher value requires major improvements. Hereof, we identify the most critical components that have the highest contribution towards system's failure. On improvements by design, the component's MDT_{c_i} can be reduced or its $MTBF_{c_i}$ can be increased. When improvements by design is not possible, adding redundancy, can increase its $MTBF_{c_i}$. After improving the component's $MTBF_{c_i}$ and MDT_{c_i}, we can again start with the reliability and availability calculations to obtain new system and component metrics. We again check the system's compliance in the designed risk matrix. This step is a recurring one, where steps 3 and 4 are repeated until the system complies to the acceptability criteria.

***Step 5* → Risk computation and prioritization**

Finally, when a system design that complies to its performance requirements is obtained. The next step plots the computed risk values ($Risk_i$) of components and subsystems are plotted in the risk matrix. On doing so, we now see how the components comply to the system's performance requirements. From this plot we can analyze and assess the components criticality to the system, based on their position in the risk matrix (low, medium, high). Although manual plotting is not an issue, for better accuracy of plotting on log scales, the current research uses MATLAB. From the position of each component or subsystem on the risk matrix we can obtained its risk priorities. With the criticalities and prioritization, we can now move on to devising optimal maintenance strategies.

***Step 6* → Maintenance planning**

Although this step is not covered in this research, using the prioritization obtained from the risk matrix, maintenance strategies can be developed for each component present in the system. This provides scope for further research on innovative maintenance strategies using the concepts used in this study.

5.2 ADDITIONAL CASE STUDY – WWTP INFRASTRUCTURE

This section of the chapter provides an additional case study comprising of a wastewater treatment plant infrastructure system. One of the major considerations of steady state calculations made for the case study as shown in the research paper is followed for the report as well. The main reason behind this, is because portraying time-variant results requires showcasing large sheets of calculations and graphs for each subsystem making it difficult to understand. The time-variant values and results for the developed method can be provided upon request (Refer colophon for contact details).

***Step 1* → System and component information**

A wastewater treatment plant (WWTP) is an infrastructure system whose principal purpose is to revamp the waste water obtained from households and public properties. Each infrastructure has a specific set of functions to perform other than their primary purpose of construction. For every asset owner, it is necessary that they get maximum returns for these up-scale investments. Therefore, to ensure they obtain the required ROI, certain performance requirements (or) service level agreements (SLA) are established by the asset owners. The SLA depicts the required operational reliability of infrastructures required by the asset owners. The designs and proposals put out by contractors and design firms are expected to conform to these requirements.

For the case study in this report, a standard service level agreement (SLA) is adopted to describe a system's requirement from an asset owner's perspective. The SLA specifications are,

- The infrastructure must have an availability of 99.9% each year including its planned downtime.
    - Remaining .1% accounts for the accidental or unforeseen downtimes that can be incurred by the system.

As we know that components fail no matter how accurate the interventions are, strategies must be developed such that the unforeseen failures conform within the tolerable limit (0.1%). Hence considerations must be made while setting up acceptability limits for checking the system's compliance and its composite component's criticality.

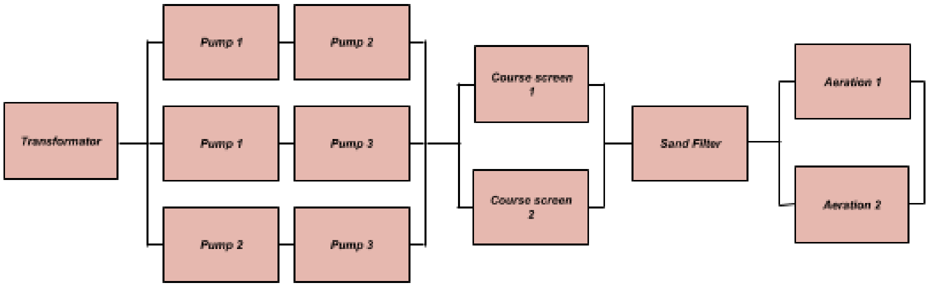

Figure 8 RBD of WWTP

The WWTP infrastructure is based on a simple treatment plant designed based on a few basic assumptions made. The system is decomposed using information on a typical WWTP design (Hannah & et.al, 2012). WWTP consists of different individual components and subsystems in a serial configuration. The system is visualized using a reliability block diagram as shown in Figure 8. Hence, upon failure of a single component or subsystem, the system fails. This makes the system to have a stricter maintenance planning to ensure the system is available as per the asset owner's requirements. To obtain information on the system's internal build, Table 6 provides the basic information on each individual component (λ_{c_i}, MDT_{c_i}) present in the system.

Table 6 Basic component data

Components	λ_{c_i}	$MTBF_{c_i}$	MDT_{c_i}
	(hours-1)	$(1/\lambda_{c_i})$ (years)	(hours)

1. Transformator	2.28E-06	50.07	12
2. Pump	7.60E-05	1.50	24
3. Course screen	2.28E-05	5.00	12
4. Sand filter	3.00E-06	38.05	36
5. Aeration	1.43E-05	8.00	24

Step 2 **→ Risk matrix design**

From the basic information on system requirements, we can now design a risk matrix for its system. The risk matrix is designed based on an iso-risk method identified from the literature study (Refer chapter 4). The scales used for RM in this research are logarithmic. For a higher accuracy in design for logarithmic scales, MATLAB was used, but the risk matrix can also be designed manually. To include SLA in the risk matrix, acceptability levels are defined based on performance requirements. With 0.1% of the planned downtime (i.e.) 8.76 hours each year, an assumption is made that components having a risk value ≥ 8.76 is critical for the system. This helps us in tracing components whose failure has an influence of crossing the 0.1% limit. Hereof, we define the minimum constant risk value ($R_0 = 8.76$) above which components become unacceptable or critical (dashed line). Similarly, we assume that components with a risk value ≤ 1 and $R_0 = 1$ is the maximum acceptable or non-critical (dotted line) risk. The portion lying amid these lines is the intermediate risk zone where components falling within this zone requires a better maintenance. Risk matrix designed for the case study is as shown in Figure 8.

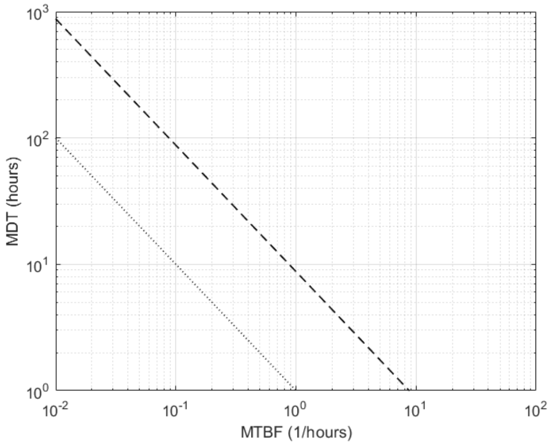

Figure 9 RM for the case study

Step 3 → Reliability and availability calculations

Next, we move on to calculating the different component and system metrics that provides the required quantitative information to check the system's compliance. The systematic approach for RA calculations as explained in the research paper (Chapter 4), is followed meticulously for each subsystem and moved up to the highest level (system). Using the failure rates (λ_{c_i}) and repair rate of each component ($\mu_{c_i} = 1/MDT_{c_i}$), (from Table 6) the steady availabilities (A_{c_i}) of each component is calculated. Once the availability of each component and subsystems are obtained, we can now estimate the system's availability (A_s). The formula to determine subsystem and system availability, conforms the reliable-path sets approach (Equation 3) based on its configuration. Using the calculated availabilities, we can now determine the sensitivity of each component in the system using the Birnbaum's conditional availability (Equation 4). From the values obtained we can identify that, components having higher BIF value to be the most sensitive to changes.

Using the A_c and instantaneous failure rate (λ_{c_i}), we can calculate the w_{c_i}, rate of occurrence of failures ($ROCOF_{c_i}$), for each component. On obtaining the unconditional intensities of each component, we now move on to estimate the system's unconditional failure intensity $w_s(t)$ using the $BIFs$ and w_{c_i} of each component. This can be done as shown in Equation 6. On obtaining the subsystem's unconditional failure intensity, we can now estimate the conditional failure rate or Vesley failure rate (λ_{vs}) using the w_s and the corresponding system's A_s as given in Equation 7.

Table 7 Calculations of each component

Components	A_{c_i}	A_s	BIF_{c_i}	CIF_{c_i}	w_{c_i} (hours-1)
Transformator	1.000E+00	0.9999726	0.9999659	0.18807	2.280E-06
Pump 1	9.982E-01	0.9999901	0.0036346	0.04549	7.586E-05
Pump 2	9.982E-01		0.0036346	0.04549	7.586E-05
Pump 3	9.982E-01		0.0036346	0.04549	7.586E-05
Course screen 1	9.997E-01	0.9999999	0.0001320	0.00025	2.282E-05
Course screen 2	9.997E-01		0.0001320	0.00025	2.282E-05
Sand filter	9.999E-01	0.9998920	0.9999717	0.74233	3.000E-06
Aeration 1	9.997E-01	0.9999999	0.0003423	0.00081	1.426E-05
Aeration 2	9.997E-01		0.0003423	0.00081	1.426E-05
System	A_s	0.9998545			
	λ_{vs}	$MTBF_s$	MDT_s		
	6.123E-06	1.633E+05	23.76		

This different steady state values are obtained for each factor of the RA calculations are provided in Table 7. From the values obtained for different BIF_{c_i} values, we can see the issue of close values as discussed in section 3.1 of the research paper. This makes differentiation of components difficult and is caused due to the negligence of considering a basic event. This is one of the major reasons why using $BIFs$ as a measure for importance was not recommended in the current research.

Now that we have all the required component metrics, we can now estimate its importance to the system. The CIF_{c_i} is calculated using the components' BIF_{c_i} and unavailability $(1 - A_{c_i})$ with a constant basic event of system unavailability $(1 - A_s)$ conform to Equation 12. From the $CIFs$ obtained we can identify the components that hold a highest importance in the system (i.e.) the component having the highest influence for a system failure. The CIF values for each component can be seen as shown in figure 6. On obtaining these metrics we can now check the system's compliance to the SLA. . The importance of each component and subsystem can be calculated using Equation 12. From the above calculations we obtain the component and subsystem's metrics which are $MTBF_{c_i}$, MDT_{c_i} and CIF_{c_i} for criticality assessment.

Table 8 Risk assessment (developed method)

Components and subsystems	**Effect Analysis**			**Criticality (Designed RM)**
	CIF_{c_i}	MDT_{c_i}	$Risk_i$	
1. Transformator	0.18807	12	2.25	Medium
2. Pump	0.04549	24	1.09	Medium
3. Course screen	0.00025	12	0.003	Low
4. Sand filter	0.74233	36	26.72	High
5. Aeration	0.00081	24	0.019	Low

From the obtained values, we can now calculate the $MTBF_s$ and MDT_s of each subsystem using their respective average hazard rate as $\frac{1}{\lambda_{vs}}$ and Equation 14. The required metrics of a system is can be derived from the values obtained for the $MTBF_s$ and MDT_s. The values of different metrics obtained are tabulated as shown in Table 8. The risk values of each component are calculated using Equation 12.

Step 4 → Check for system's compliance

To check the system's compliance to the performance requirements, using the MDT_s and $MTBF_s$ we can plot the system in the designed RM. With an $MDT_s = 23.76\, hours$ and $MTBF_s = 18.64\, years$, as shown in Figure 9. From the Figure 9, we can see that the system does not hold a position in the acceptable zone and lies in the intermediate zone.

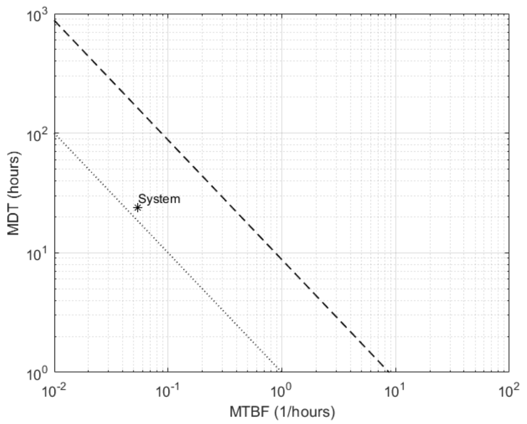

Figure 10 System compliance

Hence, it is evident that the system does not comply with the performance requirements and needs improvement. Since it falls in the intermediate zone, with a few improvements in design and redundancy of critical components the system can be brought into compliance. Looking at the $Risk_i$ values obtained, we can identify that the sand filter, Transformator and pumps hold the highest risk values among all components. To reduce impacts of these components, we need to analyze how its state within the system can be improved.

Table 9 Calculations for each component (after changes)

Components	A_{c_i}	A_s	BIF_{c_i}	CIF_{c_i}	w_{c_i} (hours-1)
Transformator	1.000E+00	0.9999863	0.9999659	0.21590	1.142E-06
Pump 1	9.989E-01	0.9999961	0.0036346	0.06532	5.701E-05
Pump 2	9.989E-01		0.0036346	0.06532	5.701E-05
Pump 3	9.989E-01		0.0036346	0.06532	5.701E-05
Course screen 1	9.997E-01	0.9999999	0.0001320	0.00057	2.282E-05
Course screen 2	9.997E-01		0.0001320	0.00057	2.282E-05
Sand filter	1.000E+00	0.9999543	0.9999717	0.71963	1.522E-06
Aeration 1	9.997E-01	0.9999999	0.0003423	0.00185	1.426E-05
Aeration 2	9.997E-01		0.0003423	0.00185	1.426E-05
	A_s	0.9999366			
System	λ_{vs}	$MTBF_s$	MDT_s		
	3.301E-06	3.029E+05	19.22		

As a part of improvements for the system, assuming that their new designs have an increased $MTBF$ and lower repair time or MDT. After changes have been made, the component data is as provided in the Table 4. To ensure that the infrastructure functions in accordance to the SLA, post changes being made. RA calculations are carried out for the system again and checked for its compliance in the RM. Using the $MDT_s = 19.22\ hours$ and $MTBF_s = 34.58\ years$, we can now check its compliance. From the RM (Figure 6), we can see that the system now holds a position in the acceptable zone. After changes we can see that the system now complies with the SLA and move to assessing the composite components.

Table 10 Risk assessment after changes (developed method)

Components and subsystems	Effect Analysis			Criticality (Designed RM)
	CIF_{c_i}	MDT_{c_i}	$Risk_i$	
1. Transformator	0.21590	12	2.59	Medium
2. Pump	0.06532	20	1.31	Medium
3. Course screen	0.00057	12	0.01	Low
4. Sand filter	0.71963	30	21.59	High
5. Aeration	0.00185	24	0.04	Low

Step 5 → Risk computation and prioritization

Now we can begin with computing the different risk values $(Risk_{c_i})$ of the components. To obtain a systematic risk assessment of each component, the FMECA technique is used as an extension for the developed method. This FMECA analyzes the different failure modes of a component (although not done in the current research) and its respective $Risk_{c_i}$ on the system. Risk assessment template for a basic FMECA incorporating the developed method is shown in Table 9.

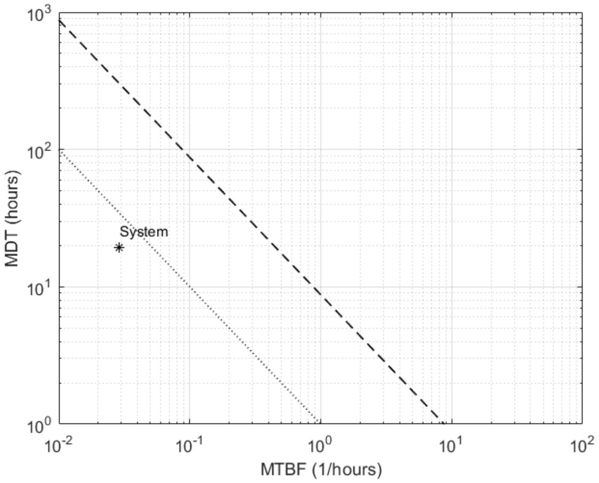

Figure 11 System compliance (after changes)

The $Risk_{c_i}$ of each component and subsystem can be calculated using their respective MDT_{c_i} and CIF_{c_i}. The values are then plotted in the designed RM as shown in figure 8. Plotting in the RM was done in MATLAB for accuracy reasons using the code given in the research paper (Chapter 4). Criticality of each component can be seen from appendix B. For instance, the Transformator has a $Risk_{c_i}$ of 2.59 is plotted in the intermediate zone. From its λ_{c_i}, we can compute the time for its first or next failure ($MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$), which is 100 years. Using its $MTBF_{c_i}$, a maintenance interval with a suitable confidence interval can be decided. Similarly, each component is assessed, and their maintenance strategies are planned based on its $Risk_{c_i}$ and $MTBF_{c_i}$.

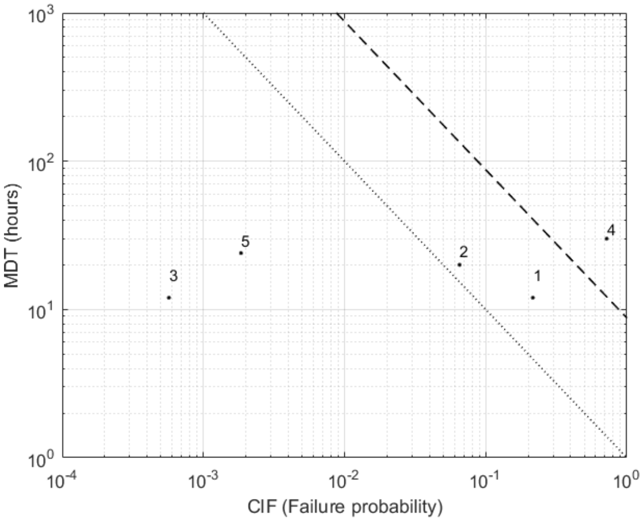

Figure 12 Plotting components in the designed RM

Step 6 → Maintenance planning

Using the prioritization and $MTBF_{c_i}$ of each component the development of a well prioritized maintenance strategy can be done (Not shown here).

Conventional method

As mentioned earlier, the case study consists of a comparative analysis with the conventional method. Hence, for the same basic component data (λ_{c_i} and $MTTR_{c_i}$) as mentioned in Table 6 and assumptions made in the system decomposition, a conventional risk assessment is performed for each case. In the conventional method, we assess criticalities based on an assumption that all components and subsystems fail at their $MTBF_{c_i} = \frac{1}{\lambda_{c_i}}$. The impact produced is equal to their MDT. We now plot the risk values following the typical interference of a criticality (i.e.) $Risk = MTBF * MTTR$. Criticality of each component is derived from the conventional RM as shown in Table 6 of this report. The scales used in this RM are linear where each cell comprises a range of values. Usually such RM are designed for different functional loss incurred by the system upon a component's failure. For instance, to assess the risk of a pump, we know from Table 2, that the pump has a redundant configuration based on the condition that 2 out of 3 pumps must function. Upon failure, the system loses 0% of its functionality. Now the component is plotted based on its $MTBF$ (1.5 years) and $MTTR$ (24 hours) in RM-3. We assign the criticality value of the entire cell, making it non-critical to the system. Similarly, each component's criticality is assessed based on the RBD, component metrics such as $MTBF$ and $MTTR$ using the RM. The conventional risk assessment method is as shown in Table 6.

Table 11 Risk assessment (conventional method)

Components and subsystems	**Effect Analysis**			**Criticality (Conventional RM)**
	$MTBF_{c_i}$	MDT_{c_i}	$Risk_i$	
1. Transformator	50.07	12	600.82	High
2. Pump	1.50	24	36.05	Low
3. Course screen	5.00	12	60.00	High
4. Sand filter	38.05	36	1369.86	High
5. Aeration	8.00	24	192.00	High

SUB-CONCLUSION

This chapters bolsters the research work showcased in chapter 4 in the form of a standalone paper. The simplified methodology provides a detailed explanation on each step of the new approach. The additional case study validates the developed method in addition to the case study provided in the paper. The following chapter comprises a detailed discussion on the results of the case study and the various research findings.

Discussions and Recommendations

The current research attempts to bridge the research gap for the problem identified with risk assessment in FMECA technique using risk matrices. This chapter discusses the results obtained for the additional case study and the various findings of the research. This chapter initially covers a detailed comparative analysis on the results obtained for the additional case study. Following which, the different findings and limitations of the research is discussed. Based on the discussions, few recommendations are provided to improve the developed method.

Discussions on comparative analysis (case study)

From the comparative study, we get an overview of the criticalities obtained from both new and conventional methods (Tables 10 and 11). On a comparative analysis, 80% difference in criticalities obtained from both methods (refer Table 12) can be seen evidently. The developed method provides a better quantitative assessment since about 60% of the components assessed as critical in the conventional method which were actually less critical. In other words, four of the five components were overestimated as critical to the system but when assessed based on their importance (new approach) they were less critical. All components that existed as subsystems (pump, course screen and aeration) were wrongly assessed in the conventional method. A major reason for this error is the (i) neglection of a configuration's compiled importance and (ii) varying acceptability levels in the conventional risk matrix. The conventional method assesses these subsystems as individual components considering only its $MTBF_{c_i}$ and MDT_{c_i}. And based on their configuration, we qualitatively assess the functional loss that could be incurred by the system upon its failure. Each risk matrix has a different range of values and the acceptability levels vary in each level. These qualitative inputs to assess a subsystem's criticality causes overestimation.

In addition, the individual components (transformator and sand filter) were also incorrectly assessed since the conventional risk matrix does not follow an error less design and has deficiencies in it. A major error with the conventional risk matrix is its negligence of different points present within each cell having values quantitatively larger than others (Anthony (Tony)Cox, 2008). Components having similar risks, fall in the same cell and cannot be differentiated. This reduces the accuracy of plotting within each cell, hence values of the entire cell are provided. This brings in the involvement of qualitative assumptions while plotting risks.

Table 12 Comparative analysis (New vs Conventional)

Components and subsystems	Criticalities obtained	
	Developed method	Conventional method
1. Transformator	Medium	High

2. Pump	Medium	Low
3. Course screen	Low	High
4. Sand filter	High	High
5. Aeration	Low	High

Another major issue with the conventional risk matrix (Appendix A) is that it has only two criticality levels, this causes extreme variations in results. Even when a component has a value that is close to adjacent cells, they either become acceptable or critical, this is also known as risk reversal errors (Baybutt, 2016). This error is eliminated in the iso-risk design (developed method) using an intermediate risk zone. The components falling in it does not become negligible and still requires better interventions. As seen from Table 12, we can see that transformator and pumps hold an intermediate risk, whereas the conventional risk matrix plots them as critical and non-critical respectively. This is a typical example of how using an iso-risk based design overcomes such variations.

Discussions and recommendations on findings

The different findings of the research originate from the solutions obtained for each research question. The discussion follows the order of sub-research questions as given below,

(a) Which risk matrix design suits best for analysing components and subsystems?

An extensive critical literature analysis (refer Chapter 4) on the different limitations and improvements seeked out by researchers were done. From which two major methods, (i) Cox's axioms and (ii) Iso-risk method were identified to be the most appropriate for assessing infrastructure components. In order to incorporate both these methods, an iso-risk based design is made in such a way that it satisfies the three Cox's axioms. To do so, the designed risk matrix consists of an intermediate risk zone so that it achieves the required betweenness in it. Using the iso-risk method, each point is separated based on constant risk values, each point is quantitatively different from each other. In addition, to complement the iso-risk design logarithmic scales were used to increase accuracy of assessing infrastructure components that have a failure rates of high order. This brings down the issues seen in the conventional risk matrix as discussed in the case study results. The current research uses MATLAB for designing the iso-risk matrix. Although it can be done manually, using this tool can make life easier and also obtain greater accuracies.

(b) What is the standardized procedure to perform RA calculations for repairable systems based on IEC 61708 norms?

The procedure to perform system calculations following the process shown in the paper (Chapter 4) is based on valid international standards IEC 61708:2016. Two points of discussion arises in its practical application. (i) Since the equations are in a time-variant form, the required period of calculations depends upon the choice of experts performing these calculations. The various factors involved in the RA calculations namely A_s, w_s, λ_{vs} and CIF_{c_i} , when modelled provides asymptotic distributions. Hence the asymptotic values depend upon the range of accuracy set by the expert's judgement. (ii) When such calculations are performed for complex systems having several individual components and subsystems, additional care is required while performing calculations. Each subsystem should be calculated before moving on to higher levels. Especially, when subsystems have different components present in it, the A_s, λ_{vs} and MDT_s (where, s is the subsystem) must be modelled and used in the system level RA calculation. Hence, a good flow map for calculation is required to obtaining accurate results for complex systems.

(c) *How can interdependencies and importance's of each component within a system be determined? and,*
(d) *What is an effective incorporation of obtained quantitative inputs for risk assessment in FMECA to develop optimal maintenance strategies?*

To determine a component's state in the system based on its interdependencies and importance, the developed method uses three main component metrics derived from the system calculations. MDT_{c_i}, CIF_{c_i} of each component and subsystem provides the required quantitative information on its state in the system accounting for its interdependency and importance in the system. The CIF_{c_i} provides the importance of a component based on a conditional failure probability and the MDT_{c_i} gives the impact of its failure. This gives a much better estimation than considering each component as individual and estimate their risks using its MDT_{c_i} and $MTBF_{c_i}$ as done in conventional methods. The developed method uses Lambert's importance factor (CIF_{c_i}) and the mean downtime (MDT_{c_i}) to compute risk values ($Risk_i$) of each component. This prioritises components based on their probability of failure as well as their importance to the system. This helps in solving the next major issue identified with the way component risks are computed and prioritised. The $MTBF_{c_i}$ of a component and subsystem gives the probable time for the first and next failure. $MTBF_{c_i}$ gives an idea on the required maintenance intervals for each component. It is defined based on a fitting confidence interval. Using the computed $Risk_i$ and $MTBF_{c_i}$ values innovative maintenance plans and strategies can be developed.

Although the line of reasoning for using MDT_{c_i} and CIF_{c_i} to compute risks are well-substantiated in the current research. A point of recommendation to improve the solution for the above-mentioned questions can be the identification of a better incorporation process using unique component metrics. New importance measures being developed in future that are appropriate to component assessment can be considered as an extension to the developed method. To develop optimal maintenance strategies the current research provides the required quantitative data. A further study on new innovative maintenance strategies can be developed using the quantitative indicators. For instance, a cost-effective maintenance plan, providing interventions only for component's having high importance.

(e) *How can the risk matrix designed from a systems' perspective provide criticalities of components and subsystems?*

One of the major purposes of the research is to eliminate the error of assessing components using a risk matrix designed from a system's perspective. The current research uses the SLA or performance requirements of an infrastructure to overcome this issue. The SLA is incorporated in the risk matrix by deriving constant risk values (R_0) for obtaining different acceptability limits. Since the developed method, initially checks a system for its compliance to the SLA, it is possible to see whether the system's typical design conforms to the required operational reliability of the asset owner. If not, the system is improved until it complies to these requirements. Hence, this process first checks the system to the SLA and then its composite components. On doing so, we check a components compliance to the same acceptability limit which the system has to obey. This helps in analysing the components having a risk that can push the system to a critical position. This eliminates the issue of analysing components from a system's perspective.

From the above discussions and recommendations, a short picture into how the current research can be extended with further study can be obtained.

Conclusion

To conclude, an elaborate solution for the framed main research question would provide a holistic closure for the entire study.

"What is an optimal risk assessment approach in FMECA to obtain accurate criticalities of repairable components present in an infrastructure system?"

The new risk assessment approach obtains criticalities of components using quantitative data derived from repairable system reliability and availability calculations. The different component and system metrics obtained are then incorporated into an asset specific risk matrix designed based on SLA of the infrastructure. On plotting each component using metrics such as CIF_{c_i} and MDT_{c_i}, their risk levels and accurate criticality to the system is defined. The asset-specific risk matrix assesses criticalities of components based on their compliance to the performance requirements of the system. Since the system is improved until it complies to the performance requirements, the components with the highest risk can very well be interpreted as the ones that have a higher contribution towards non-compliance of the system. Hence, the new risk assessment approach provides optimal criticalities of components in a system eliminating the various issues identified initially.

To get here, this thesis report starts with an explanation on the problem identified in FMECA's application of risk matrices. The problem illustration and analysis provided in chapter 2 gives an overview on the problem's existence in practice. The problem analysis deduced the several limitations and neglections present in the conventional method. Based on which, three major quantitative information required to improve the existing method were realized. They are, i) number of similar components present within the system, (ii) type of configuration and (iii) importance of a component or a subsystem to the infrastructure.

The current research follows a pragmatic methodology that can entail a combination of both qualitative and quantitative study. A meticulous research design was made showcasing the different research questions, objectives and methodology. On following the research design, it was possible to obtain the desired results with minimum deviations. The next steps of the research endeavoured in acquiring solutions for the different questions framed aimed to be applied on real-time case studies.

Initially an extensive critical literature analysis was performed. The literatures chosen for this analysis comprised of articles that covers the different issues present in the risk matrix tool. Following which a detailed analysis on the various improvements and developments endeavoured by researchers on the risk matrix techniques was performed. Among the several methods available, an iso-risk design method was chosen, and a risk matrix was developed in such a way it satisfies the three axioms of Cox. The risk matrix designed for the new approach uses logarithmic scales and asset specific acceptability limits.

From the reliability and availability calculations, it was possible to derive several system and component metrics. These metrics could provide assessments on whether the components and subsystems comply to the infrastructure's requirements. The system metrics $MTBF_S$ and MDT_S are plotted in the designed risk matrix to check if the system complies to the requirements and improved internally until it does. Once the system complies, the different components and subsystems are assessed using their CIF_{c_i} and MDT_{c_i}. The risk values $(Risk_i)$ are then used to prioritise each component and maintenance intervals are based on its $MTBF_{c_i}$.

The developed method was then applied along with the conventional approach on two infrastructure cases for a comparative study. The results of this research were affirmative and showcased that the new approach provided an improved assessment than the conventional method. This led to writing the research in the form of a standalone paper with an aim of publishing in targeted journals. The latest version of the paper written formed the content of the research in this report. To bolster the content, a simplified methodology providing a detailed explanation on the new approach and an additional case study was provided.

The wrap-up of the entire research follows the conclusion given in the research paper. The new developed method provides an improved quantitative analysis on the components present within a system than the conventional method. From the two-case studies it was evident that the maintenance plans developed using the new approach will be highly reliable. Since the research not only solves the problem identified, it also adds value to the existing FMECA approach making it a much better tool in the fields of Infrastructure asset management.

References

A.Glerum, & A.Vrijburcht. (2000). Design of Locks. *Directorate General of Public Works Civil Engineering Division, Bouwdienst Rijkswaterstaat*, (ISBN 90-369-3305-6).

Anthony (Tony)Cox, L. (2008). What's Wrong with Risk Matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Antosz, K., Stadnicka, D., & Ratnayake, R. M. C. (2017). Development of a risk matrix for the assessment of maintenance suppliers: A study based on empirical knowledge. *IFAC*, *50*(1), 9026–9031. https://doi.org/10.1016/j.ifacol.2017.08.1586

Arunraj, N. S., & Maiti, J. (2007). Risk-based maintenance—Techniques and applications. *Journal of Hazardous Materials*, *142*(3), 653–661. https://doi.org/https://doi.org/10.1016/j.jhazmat.2006.06.069

Aschauer, D. A. (1990). Why Is Infrastructure. *Transportation Research Board*, pp 21-68.

Bahill, A. T., & Smith, E. D. (2009). *An industry standard risk analysis technique*. *EMJ - Engineering Management Journal* (Vol. 21).

Bao, C., Wu, D., Wan, J., Li, J., & Chen, J. (2017). Comparison of Different Methods to Design Risk Matrices from The Perspective of Applicability. *Procedia Computer Science*, *122*, 455–462. https://doi.org/10.1016/j.procs.2017.11.393

Baybutt, P. (2015). Calibration of risk matrices for process safety. *Journal of Loss Prevention in the Process Industries*, *38*, 163–168. https://doi.org/10.1016/j.jlp.2015.09.010

Baybutt, P. (2016). Designing risk matrices to avoid risk ranking reversal errors. *Process Safety Progress*, *35*(1), 41–46. https://doi.org/10.1002/prs.11768

Bevilacqua, M., & Braglia, M. (2000). *Analytic hierarchy process applied to maintenance strategy selection*. *Reliability Engineering & System Safety* (Vol. 70). https://doi.org/10.1016/S0951-8320(00)00047-8

Birolini, A. (2013). Reliability engineering : theory and practice. Heidelberg: Springer. https://doi.org/10.1007/978-3-642-39535-2

Buzacott, J. A. (1967). Finding the MTBF of repairable systems by reduction of the reliability block diagram. *Microelectronics Reliability*, *6*(2), 105–112. https://doi.org/10.1016/0026-2714(67)90173-4

Chybowski, L., & Gawdzińska, K. (2016). On the Present State-of-the-Art of a Component Importance Analysis for Complex Technical Systems BT - New Advances in Information Systems and Technologies. In Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, & M. Mendonça Teixeira (Eds.) (pp. 691–700). Cham: Springer International Publishing.

Dekker, R. (1996). Applications of maintenance optimization models: a review and analysis. *Reliability Engineering & System Safety*, *51*(3), 229–240.

https://doi.org/https://doi.org/10.1016/0951-8320(95)00076-3

Dhillon, B. S. (2007). Applied reliability and quality : fundamentals, methods and procedures. London: Springer. https://doi.org/10.1007/978-1-84628-498-4

Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. *Safety Science*, *76*, 21–31. https://doi.org/10.1016/j.ssci.2015.02.014

Dutuit, Y., & Rauzy, A. (2015). On the extension of Importance Measures to complex components. *Reliability Engineering and System Safety*, *142*, 161–168. https://doi.org/10.1016/j.ress.2015.04.016

Ebeling, C. E. (2005). *An introduction to reliability and maintainability engineering.* Long Grove SE - 486 blz. ; .. cm. + 1 CD-ROM.: Waveland.

Elmontsri, M. (2014). *Review of the Strengths and Weaknesses of Risk Matrices*. *The Journal of Risk Analysis and Crisis Response* (Vol. 4). https://doi.org/10.2991/jrarc.2014.4.1.6

Giorgio, B., M., F. D., & Mohamed, S. (2014). Optimization of Life-Cycle Maintenance of Deteriorating Bridges with Respect to Expected Annual System Failure Rate and Expected Cumulative Cost. *Journal of Structural Engineering*, *140*(2), 4013043. https://doi.org/10.1061/(ASCE)ST.1943-541X.0000812

Hannah, T. W., & et.al. (2012). Wastewater treatment plant design handbook. *Water Environment Federation*.

Hokstad, P. (1997). The failure intensity process and the formulation of reliability and maintenance models. *Reliability Engineering & System Safety*, *58*(1), 69–82. https://doi.org/https://doi.org/10.1016/S0951-8320(97)00053-7

IEC/ISO 31010:2009. (n.d.). Nen-ISO/IEC 31010. *International Standards for Riskmanagement - Risk Assessment Techniques, International Electrotechnical Commission (IEC).*

IEC 61708:2016. (n.d.). Nen-ISO/IEC 61708. *International Standard Reliability Block Diagrams. Geneva, Switzerland: International Electrotechnical Commission (IEC).*, (december 2016).

J.K, V. (2016). Importances of components and events in non-coherent systems and risk models. *Reliability Engineering and System Safety*, *147*, 117–122. https://doi.org/10.1016/j.ress.2015.11.007

Kapadia, J., & Llc, N. B. (2017). An Integrated System-Oriented Risk and Reliability Analysis Methodology to Improve Maintenance Strategies of Beverage Filling and Packing Line Equipment, (Cm), 824–830.

Kapadia, J., & Tabibzadeh, M. (2017). An Integrated System-Oriented Risk and Reliability Analysis Methodology to Improve Maintenance Strategies of Beverage Filling and Packing Line Equipment. *IIE Annual Conference. Proceedings*, 824–829. Retrieved from https://search.proquest.com/docview/1951120409?accountid=27026

Laurance, W. F., Peletier-jellema, A., Geenen, B., Koster, H., Verweij, P., Dijck, P. Van, … Kuijk, M. Van. (2015). impacts of rapid infrastructure expansion, 259–262.

Levine, E. S. (2012). Improving risk matrices: the advantages of logarithmically scaled axes. *Journal of Risk Research*, *15*(2), 209–222. https://doi.org/10.1080/13669877.2011.634514

Memarzadeh, M., & Pozzi, M. (2016a). Integrated Inspection Scheduling and Maintenance Planning for Infrastructure Systems, *31*, 403–415. https://doi.org/10.1111/mice.12178

Memarzadeh, M., & Pozzi, M. (2016b). Integrated Inspection Scheduling and Maintenance Planning for Infrastructure Systems. *Computer-Aided Civil and Infrastructure Engineering*, *31*(6), 403–415. https://doi.org/10.1111/mice.121780

Moubray, J. (1997). *Reliability-centered maintenance*. *TA - TT* - (2nd ed.). Oxford SE - xv, 423 pages : illustrations ; 24 cm: Butterworth Heinemann.

Novozhilov, E. O. (2015). Guidelines for construction of a risk matrix. *Functional Safety. The Theory and Practice*, 80–86.

Peace, C. (2017). The risk matrix: Uncertain results? *Policy and Practice in Health and Safety*, *15*(2), 131–144. https://doi.org/10.1080/14773996.2017.1348571

Pickering, A., & Cowley, S. (2010). *Risk matrices: Implied accuracy and false assumptions*. *Journal of Health and Safety Research and Practice* (Vol. 2).

Purba, J., & Deswandri, D. (2018). *The Implementation of Importance Measure Approaches for Criticality Analysis in Fault Tree Analysis: A Review*. *Jurnal Pengembangan Energi Nuklir* (Vol. 20). https://doi.org/10.17146/jpen.2018.20.1.4257

Rajeev Ruparathna, Kasun Hewage, R. S. (2017). No Title. *Journal of Cleaner Production*, 1–16.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2012). *Research methods for business students*. Harlow, England; New York: Pearson.

Topuz, E. (2009). Reliability and availability basics. *IEEE Antennas and Propagation Magazine*, *51*(5), 231–236. https://doi.org/10.1109/MAP.2009.5432110

Verschuren, P. J. M., Doorewaard, H., Poper, R., & Mellion, M. J. (2010). *Designing a research project*. The Hague: Eleven International Publishing.

Yusta, J. M., Correa, G. J., & Lacal-ara, R. (2011). Methodologies and applications for critical infrastructure protection : State-of-the-art, *39*, 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

Appendix

A. Conventional risk matrix for WWTP case study

		Mean time to failure							
Risk matrix No.	Downtime Incurred	>100 years	15 ≤ 100 years	10 ≤ 15 years	5 ≤ 10 years	2 ≤ 5 years	1 ≤ 2 years	0,25 ≤ 1 years	≤ 0,25 years
RM-1	***Repair time < 4 hours***								
	Capacity reduction > 75%	░	░	■	■	■	■	■	■
	50% < capacity reduction =< 75%	░	░	░	░	■	■	■	■
	25% < capacity reduction =< 50%	░	░	░	░	░	■	■	■
	5% < capacity reduction =< 25%	░	░	░	░	░	░	■	■
	Capacity reduction =< 5%	░	░	░	░	░	░	░	■
RM-2	***Repair time 4 - 16 hours***								
	Capacity reduction > 75%	░	■	■	■	■	■	■	■
	50% < capacity reduction =< 75%	░	░	░	■	■	■	■	■
	25% < capacity reduction =< 50%	░	░	░	░	■	■	■	■
	5% < capacity reduction =< 25%	░	░	░	░	░	■	■	■
	Capacity reduction =< 5%	░	░	░	░	░	░	░	■
RM-3	***Repair time 16 - 48 hours***								
	Capacity reduction > 75%	░	■	■	■	■	■	■	■
	50% < capacity reduction =< 75%	░	■	■	■	■	■	■	■
	25% < capacity reduction =< 50%	░	░	░	■	■	■	■	■
	5% < capacity reduction =< 25%	░	░	░	░	■	■	■	■
	Capacity reduction =< 5%	░	░	░	░	░	░	░	■
RM-4	***Repair time 16 - 5 days***								
	Capacity reduction > 75%	■	■	■	■	■	■	■	■
	50% < capacity reduction =< 75%	░	■	■	■	■	■	■	■
	25% < capacity reduction =< 50%	░	░	░	■	■	■	■	■
	5% < capacity reduction =< 25%	░	░	░	░	■	■	■	■
	Capacity reduction =< 5%	░	░	░	░	░	░	░	■
RM-5	***Repair time > 5 days***								
	Capacity reduction > 75%	■	■	■	■	■	■	■	■
	50% < capacity reduction =< 75%	■	■	■	■	■	■	■	■
	25% < capacity reduction =< 50%	░	■	■	■	■	■	■	■
	5% < capacity reduction =< 25%	░	░	■	■	■	■	■	■
	Capacity reduction =< 5%	░	░	░	░	░	░	░	■

■	High
░	Low