Applying empirical method for performance metrics measurement of a nuclear security system

Maizura Ibrahim1,a), Siti Nurbayah Hamdan1, Saa’idi Ismail1, Mohamad Safuan Sulaiman1, Sufian Norazam Mohamed Aris1, Mohd Hasnor Bin Hasan1, Mohd Dzul Aiman Aslan1, Nur Fatini Abdul Ghani1 and Amy Hamijah Ab Hamid1

1Information Technology & Application Centre, Technical Support Division, Malaysian Nuclear Agency, Bangi, 43000 Kajang, Selangor Darul Ehsan, Malaysia.

a)maizura@nm.gov.my

Abstract. A nuclear security system is often developed based on a particular framework. In our case, a nuclear security system is developed based on the big data analytics framework with the purpose of integrating all nuclear security systems within a nuclear facility. Nuclear security can be defined as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities. Whereas, big data analytics is denoted as a new way of collecting, analyzing large amounts of data, finding the appropriate patterns to support decision making, hence improving the action taken in solving the problems. The system-based evaluations methodology is widely used to measure the performance metrics of nuclear security systems. However, the system-based evaluation methodology consumes time and demands a lot of effort because in applying the methodology, a complete nuclear security system that is based on the particular framework needs to be designed, developed, and implemented in the nuclear facilities environment before the performance metrics could be measured. In this paper, we present an empirical method of measuring the performance metrics by utilizing the Rasch Measurement Model. The methodology is formulated to reduce the time and efforts in measuring the performance metrics of a nuclear system that is developed based on a framework…

1. Introduction
Nuclear security is defined as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities[1]. Any system that is created and implemented to achieve nuclear security, whether it is a computer-based system or a manual system is regarded as a nuclear security system. The context of our work is derived based on a computer-based system, which in broader terms is also known as the electronic management system. Thus, the nuclear security system focused in our work is regarded as the application/software that is developed to provide the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities. Our work uses the big data analytics framework as a basis for system design[2]. We defined Big data as the high volume, high velocity, high variety, and high veracity, i.e., the 4Vs of data (information assets) that require new forms of processing, to enable enhanced decision making, insight discovery, and process optimization [3].
Several methods have been used to evaluate the performance metrics of a system, such as the system-based, theoretical-based, and hypothetical-based methodology. The system-based methodology is widely used in measuring the performance metrics of an application/software in the Information Technology field. Whereas, the theoretical-based and hypothetical-based methodologies are widely applied in measuring the performance metrics of a system in the Nuclear Security field. The system-based evaluation methodology is defined as performing several systematic processes into the final version of a system as an assessment to see whether the system has met the specified goals or not. The system-based evaluation methodology consumes time and demands a lot of effort. Therefore, in this paper, we present an empirical method of measuring the performance metrics by utilizing the Rasch Measurement Model. The methodology is formulated to reduce the time, efforts, and process complexity in measuring the performance metrics of a nuclear system that is developed based on a framework. The first section has introduced the topic addressed in this paper. The second section reveals the related works. The third section presents the proposed methodology. The section is followed by a comparison and discussion of three different methodologies that are commonly applied. The final section presents the conclusions of the paper and proposes future work.

2. Related works
This paper reports on a review of methodologies that are applied in the assessment process of a nuclear security system. In addition, this article also presents the technique of applying an empirical method in measuring the performance metrics of our work that were previously published in [2][4][5][6][7]. While the system-based methodology is commonly used to evaluate the application/software in the IT domain, the theoretical-based and hypothetical-based techniques are commonly used in the Nuclear Security domain. However, for this work, we proceed the research through the path that is commonly applied in software engineering research. In other words, we look at our research work from the perspective of an empirical research project. Therefore, for the evaluation process, the empirical method is proposed to be applied in assessing our work. The empirical method is defined as any procedure for conducting an investigation that relies upon experimentation and systematic observation rather than theoretical speculation.

The system-based methodology is widely applied in assessing an application software following a regular application development process such as software development lifecycle[8]. In system-based evaluation methodology, the application software should be designed and developed first before the assessment process could be conducted. Apart from that, the theoretical-based and hypothetical-based are commonly found in the literature related to nuclear security assessment methodologies. The nuclear security assessment methodologies and tools are designed to provide assurance that regulated facility protection measures are effective against the threat as defined in the State’s threat assessment or design basis threat. The IAEA-TECDOCS-1868 entitled the Nuclear Security Assessment Methodologies for Regulated Facilities (NUSAM) applied the theoretical-based and hypothetical-based methodology [9]. This IAEA-TECDOCS was published to provide the Member States of IAEA with a standard nuclear security assessment methodology and criteria to assist in assessment tool(s) selection. The IAEA Nuclear Security Series No. 4 entitled Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage applied the hypothetical-based methodology intending to prevent the revelation of the detailed design of the nuclear security system [10].

3. The empirical methodology for measuring the performance metrics of a nuclear security system based on big data analytics framework
The proposed empirical methodology used to evaluate the performance metrics for the big data analytics nuclear security framework is depicted in Fig. 1. The methodology outlined nine major steps. The first step is the framework that will be used as the basis for the application/software development must be developed. For the framework development methodology, we left the option open, which means any
existing methods could be adopted. The second step is the process of identifying the framework's peculiarities elements with regards to the previous nuclear security framework. In our work, the fundamental elements of our framework are based on the existing International Legal Framework for Nuclear Security, which we constituted as a non-big data analytics nuclear security framework. The International Legal Nuclear Security Framework is illustrated by the International Atomic Energy Agency (IAEA) in multiple publications of the IAEA Nuclear Security Series, staggered in four different levels of grouped materials, i.e. Nuclear Security Fundamentals [11], Recommendations, Implementing Guides, and Technical Guidance, Reference Manuals, Training Materials. Therefore, the peculiarities elements are identified as the elements that do not appear in the existing International Legal Framework for Nuclear Security. These peculiar elements are the performance metrics that are going to be measured during the evaluation process.

![Diagram](image)

**Figure 1.** An empirical method for measuring the performance metrics of a nuclear security system based on a big data analytics framework.

The third step is to identify and develop the pilot environment for the evaluations processes. This is the preliminary step taken to make sure the instrument used in the measurement, evaluation, and statistical analysis before any data collection hence data analysis, is correct and could measure what the evaluation process suppose to measure. This is a very important step that needs to be given very serious consideration because a faulty instrument will render the data useless and the data analysis is therefore null and void. During this step, the research questions are also formulated and clarified as the elementary step before the design and development of the survey questionnaire (step 4) because research design is a key element in shaping the way research questions are going to be asked in the survey questionnaire[12]. The broad research question we ask in our work is, to what extent does adopting our big data analytics nuclear security framework affect the security of radioactive materials in the Malaysian Nuclear Agency? From the broad research question, variables are identified and distinguished between three types of variables, which are dependent, independent, and intervening.

Step 4 consists of activities to design and develop the survey questionnaire based on the focus and clarified research questions, the dependent, independent, and intervening variables. Here we depict this research as a case study method because this research does not fundamentally rely on comparing cases but on fully understanding the ‘wholeness’ effect of implementing the big data nuclear security framework on securing the radioactive/nuclear materials in the Malaysian Nuclear Agency. We also consider our research questions as a descriptive type rather than an explanatory one because what we
want from the result of this survey is to describe and confirm the effect of implementing the big data nuclear security framework specifically in the Malaysian Nuclear Agency, based on the cause and effect that are theoretically mentioned in previous reports published by World Institute of Nuclear Security (WINS) [13][14]. Our survey questionnaire is developed by making use of the Google form online survey platform.

After step 4 is completed, the implementation is done by distributing the online survey questionnaire to the pilot experiment targeted individuals via email and WhatsApp messaging platform (step 5). In step 6, the result is analyzed based on the procedure outlined by Rasch Measurement Model[15][16][17]. Rasch model provides a way to evaluate the instruments used during the pilot experiment. The results obtained during the pilot experiment could be used to validate the research design. If the obtained results are acceptable, then one could proceed to the execution of step 7, step 8, and step 9. If the pilot results point out that the instrument used is not valid, the procedure in step 3 should be re-evaluated, then proceed with pilot implementation again, until the results are acceptable. We have several reasons and justification for why we propose our method for the evaluation of our work. The next section compares and discusses the reasons.

4. Methodologies comparison and discussion

Table 1 presents the result of our review process that is done to compare the empirical-based evaluation method with the theoretical/hypothetical-based, and system-based. The comparison is made based on three properties, i.e., requirements, time consumption, risk, and process complexity.

| Properties          | Empirical-Based | System-Based Evaluation Method | Theoretical / Hypothetical-Based |
|---------------------|-----------------|--------------------------------|---------------------------------|
| Requirements        | A framework that is used as the basis for the applications/systems development must be developed first. | A complete system needs to be designed, developed, and implemented in the nuclear facilities environment before the performance metrics could be measured. | A complete design of the system. Most designs are developed based on threat assessment (DBT), thus DBT must be developed first. |
| Time consumption    | Low             | Long                           | Moderate                        |
| Risk                | Low             | High                           | Low                             |
| Process complexity  | Low             | High                           | High                            |

The requirements are defined as the input that is needed to proceed with the evaluation process following each specific methodology. To start the evaluation process by following our empirical-based method, a framework that is used as the basis for the application/system development needs to be developed and ready first. Whereas, to adopt the system-based evaluation method, a complete nuclear security system needs to be designed, developed, and implemented in the nuclear facilities before the evaluation process could be started. Apart from that, to evaluate the nuclear security system following the theoretical/hypothetical-based methodology, a complete system design based on threat assessment (Design Basis Threat) needs to be ready before the evaluation process could be initiated. Therefore, requirements for implementing empirical-based methodology constitute low time consumption, low risk, and low process complexity. However, we regard the system-based evaluation method consumes a long time due to the requirement of system design, development, and implementation that commonly take a very long time to be finished. Hence, the risk of applying this method is regarded as high because if the system development fails, the chances of failing to obtain the performance evaluation result are very high. Thus, the context of risk here meant the risk of not being able to start the evaluation process.
due to the fail of preparing their requirements. Meanwhile, the context of process complexity in this paper is regarded as the overall process from preparing the requirements until the evaluation is finished. Since the system-based evaluation method and the theoretical/hypothetical-based method require more than one stage of preparation before the evaluation process could be initiated, they are regarded as a high complexity process compared to the empirical-based method which only needs a framework preparation (one stage only).

5. Conclusion and future works
In this paper, we had proposed an empirical methodology to evaluate the performance metrics of a computer-based nuclear security system that is developed based on the big data analytic framework. The key element of this methodology is that this methodology is developed by applying the empirical method, so there will be no probabilistic assessment involved. Besides, the implementation process is straightforward and could be done by distributing and collecting the result via the online survey questionnaire, thus, it could be re-implement on any online survey platform. The design of the survey and analysis is done by applying Rasch Measurement Measure Model, which constitutes a precise cycled evaluation. This methodology has low time consumption, low risk, and low process complexity compared to the previous methodologies such as system-based, theoretical-based and hypothetical-based methodology. Our future works are to implement the proposed methodology after the method validation process is done by the expert in our research collaboration team members.

6. References
[1] International Atomic Energy Agency 2008 Security in transport of radioactive material, implementing guide IAEA Nuclear Security Series No.9. (Vienna, Austria).
[2] Ibrahim M, Ismail S, Haris M F, Hamdan S N, Sulaiman M S, Hamid A H A, Aris S N M, Aslan M D A, Ghani N F A, and Hassan H 2021 Big Data analytics nuclear security framework, IOP Conf. Ser.: Mater. Sci. Eng. 1106 012026
[3] Beyer M A and Laney D 2012 The importance of big data: A definition (Stamford, CT: Gartner).
[4] Ibrahim M, Ismail S, Haris M F, Hamdan S N, Sulaiman M S, Hamid A H A, Aris S N M, Aslan M D A, Ghani N F A, and Hassan H 2017 2017 A proposal on adaptation of big data analytics framework in nuclear security toward development of integrated, real-time, and intelligent nuclear security system, Nuclear R & D Seminar, Selangor, Malaysia.
[5] Ibrahim M, Ismail S, Haris M F, Hamdan S N, Sulaiman M S, Hamid A H A, Aris S N M, Aslan M D A, Ghani N F A and Hassan H 2018 The integrated intelligent nuclear security (I2NS) system: A progress report for 2018, Technical Report No.NUKLEARMALAYSIA/L/2018/173 (Kajang, Selangor, Malaysia: Malaysian Nuclear Agency).
[6] Ibrahim M, Ismail S, Haris M F, Hamdan S N, Sulaiman M S, A. H. A. Hamid, S. N. M. Aris, M. D. A. Aslan, N. F. A. Ghani, and H. Hassan 2020 Malaysian Nuclear Agency integrated & intelligent nuclear security (I2NS) system: A progress report 2019 Technical Report No.NUKLEARMALAYSIA/L/2020/10 (Kajang, Selangor, Malaysia: Malaysian Nuclear Agency).
[7] Ibrahim M, Ismail S, Haris M F, Hamdan S N, Sulaiman M S, Hamid A H A, Aris S N M, Aslan M D A, Ghani N F A and Hassan H 2020 Big data analytics for nuclear security: A literature review, Nuclear R & D Seminar 2020 16th – 19th November 2020, Kajang, Selangor, Malaysia.
[8] Unit Pemodenan Tadbir dan Perancangan Pengurusan Malaysia (MAMPU) 2019 KRISA: Kejuruteraan sistem aplikasi sektor awam-satu panduan komprehensif dan praktikal, (Putrajaya, Malaysia: MAMPU).
[9] International Atomic Energy Agency (IAEA) 2019 The nuclear security assessment methodologies for regulated facilities (NUSAM) IAEA-TECDOCS-1868 (Vienna, Austria).
[10] International Atomic Energy Agency IAEA 2007 Engineering safety aspects of the protection of nuclear power plants against sabotage IAEA Nuclear Security Series No.4 (Vienna, Austria).
[11] International Atomic Energy Agency (IAEA) 2013 Objective and essential elements of a state’s nuclear security regime, nuclear security fundamentals IAEA Nuclear Security Series No.20 (Vienna, Austria).

[12] David de Vaus 2002 Surveys in social research 5th ed (NSW, Australia: Allen & Unwin).

[13] World Institute of Nuclear Security (WINS) 2015 Data analytics for nuclear security, how real-time integrated data management could support nuclear security WINS Special Report Series, January 2015 (Vienna, Austria).

[14] World Institute of Nuclear Security (WINS) 2015 Big data in motion, how real-time integrated data management could support nuclear security WINS Special Report Series, September 2015, (Vienna, Austria).

[15] Bond T G and Fox C M 2015 Applying the Rasch model: Fundamental measurement in the human sciences 3rd ed. (Routledge, NY, US: Taylor & Francis Publishers).

[16] Wright B. and Mok M 2004 An overview of the family of rasch measurement models, in introduction to Rasch measurement: theory, models, and applications ed Everett J, Smith V and Smith R M.

[17] Wright B D and Stone M H 1999 Measurement essentials 2nd ed (Wilmington, Delaware, USA: Wide Range, Inc).

Acknowledgments
This study is supported by the International Atomic Energy Agency (IAEA) research grant under the IAEA Coordinated Research Project CRP J02011: Improving the Security of Radioactive Material throughout its Lifecycle, Associated Facilities, and Associated Activities (Contract No. 22165).