

# Electromagnetic Warfare Intentional Interference: Victim Risk Assessment.

Nigel Davies, Chris Williams, Mark Osborne, Huseyin Dogan, Duncan Ki-Aries and Nan Jiang

**Abstract** - Preventing an adversary's Electromagnetic (EM) equipment from fully functioning via "Intentional Electromagnetic Interference" (IEMI) is strategically beneficial but technically complicated because optimal decisions on emitted signal frequency/power require unknown/unknowable knowledge of target systems' EM architecture. Further complications are complex EM environment topologies and target location uncertainty. Additionally, IEMI aimed at targets is somewhat indiscriminate because emitted signals potentially interfere with non-target EM systems (e.g. civilian or allied), called victims. Determining the appropriate IEMI target-focussed signal emission strategy, involves complicated decision-making processes involving comprehending victim risks. This requires a Quantitative Risk Assessment Method (QRAM). This article describes the development of a novel QRAM utilising a Monte Carlo technique for calculating probabilities of degradation to victim systems to calculate victim risk within complex, dynamic, uncertain environments, potentially enabling risk-informed decisions on attack options. Its novelty is the combination of methodologies, with an approach extending beyond merely physical aspects (i.e. propagation of EM waves, or their physical interaction with individual systems), to include other critical aspects, allowing generation of simple metrics representing the likely consequence, in a context that can be directly exploited by decision makers.

**Index Terms** —Risk Assessment; Intentional Electromagnetic Interference; Systematic Review; Monte Carlo Mathematical Modelling; Verification Testing.

N. Davies, H. Dogan, D. Ki-Aries and N. Jiang are with Bournemouth University, UK. C. Williams and M. Osborne are with DSTL.

## I. INTRODUCTION

**M**ILITARY operations are broadly split into planning and execution. During execution, communication between allied participants is essential and applies Electromagnetic Spectrum Operations (EMSO), so control over adversary communications systems using "Intentional Electromagnetic Interference" (IEMI) is strategically beneficial. However, the battle for such control has associated risks to non-adversary systems (called victims) e.g. allied military or civilian systems. Some victim risks may be

unacceptable (or acceptable) to an attacker (when taking account of the law of armed conflict), so knowledge of victim risks is an essential input to decision-making. Attackers should thus perform an appropriate victim Risk Assessment (RA). Typically, RA is performed by those who are responsible for controlling hazards, which are usually the owners (who we might call defenders) of a vulnerable system. RA is therefore usually considered from such a defender's perspective, not an attacker. For example, RA is performed in the domain of Safety Risk Management (RM) [1] where potential harms are defined as hazards with Hazard Identification and Analysis methods [2] such as Hazard and Operability Studies (HAZOP) [3], Failure Modes and Effects Analysis (FMEA) [4], Fault Tree Analysis (FTA) [5], Event Tree Analysis (ETA) [6] and Bow-Tie Analysis [7] applied to determine likelihood of harms to vulnerable people/systems, to provide input to the RA process. Of course, the principles of RA do not only apply to the domain of Safety RM but also apply to a variety of other contexts (e.g. defending cyber systems from hackers). This is highlighted within the ISO standard ISO31000 [8] where the establishment of context is the primary task in the overall RM process. So, while some forms of RA are performed by potential victims of harm, because it is focused on a defender's decision-making process and not on that of an attacker, an IEMI victim RA process is required to calculate risk associated with victim systems representing collateral interference from an attacker's perspective. This nuanced difference requires the adoption of a new approach to the utilisation of RA, and the adaption of existing techniques to this different perspective. A key challenge resulting from this difference in perspective is there is a high degree of uncertainty: firstly, whether a victim exists in a specific location and secondly about what level of impact an attacker might have on a victim, whereas from a defensive perspective there is clearer knowledge of location and potential victim impact measures.

The purpose here is to report on the development of an appropriate Quantitative Risk Assessment Method (QRAM) and its application to IEMI. This is formative work, so has used simple examples of IEMI, and employed simple physics models to make the work practically achievable using the compute power available to the research project. The QRAM has the capability to calculate risk to victim systems within complex, dynamic, uncertain environments

aimed at facilitating military commanders in making risk-informed decisions on IEMI attack options. A description of IEMI is provided in section II for readers unfamiliar with this RM context, which also explains victim risks in more detail. The systematic review is summarised in section III while section IV describes the QRAM's mathematical modelling foundations. The research reported here is focussed on the overall approach to victim RA and the application of the QRAM to support EM transmission decision making, so the focus is not on the level of fidelity of physical models or modelling of EM interactions per se (although future work could improve these). With this in mind, a relevant program of verification testing is described and discussed in section V covering results and analysis of appropriate tests. Conclusions and suggested further work are in section VI. Throughout the article there are many acronyms which are listed in a glossary in section VII.

## II. IEMI

EMSO: “*are military actions to exploit, attack, protect, and manage the electromagnetic operating environment*” [9]

EMSO includes degradation of adversaries' EM equipment to prevent them from fully functioning using interference via the transmission of EM signals, i.e. IEMI [10]. Adversary systems (to which IEMI is targeted) are defined here as “targets”. However, such attempts cannot guarantee successful achievement of the attacker objectives on the target systems because IEMI relies upon factors such as successfully penetrating shielding technologies and attaining directionally correct, sufficient power at appropriate signal frequencies. Attempting IEMI is also technically complicated because optimal decisions on emitted signal frequency/power require knowledge of the target architecture which is comprised of many varied interdependent subsystems of EM components (often unknown/unknowable). During EM interactions within EM environments there can be significant numbers of EM couplings, propagations and effects, some of which (a potentially random quantity) are outside a component's intended operating limits. For an attacker, the hope is that these will sufficiently degrade an adversary's system although the impact on it causes potentially indeterminate system effects. IEMI is further complicated by target location uncertainty within complex EM environment topologies. Additionally, IEMI aimed at targets is somewhat indiscriminate because emitted signals may also interfere with non-target EM systems (e.g., civilian or allied), as mentioned above. These victims also have associated architecture/location uncertainties and impact on victims is also victim-system multi-component-state dependent.

Models of both target and victim systems (assuming sufficient knowledge exists) can be

constructed using methods such as HAZOP, FTA, etc., which may aid analysis of victim system interference. However, an additional complicating, contrasting, distinction between using Hazard Identification methods within an IEMI context and (say) a Safety RM context is that within a Safety RM context the primary aim is singularly avoidance of damage (determined through assessed risk from hazards). In IEMI, the attacker's aim is not singular, it is twofold. Whilst (like safety RM) avoidance of interference to victim systems is a risk-informed consideration – the intent is to cause equipment interference within potentially an unknown (and/or unknowable) target structure in an unknown (and/or unknowable) state while simultaneously considering the risk of interference to victims. So, in the IEMI context, RA is not focused only on a defender's perspective.

The risk to victims from this interference may (or may not) be acceptable to an attacker (as also previously mentioned), therefore, determining the appropriate IEMI target-focussed signal emission strategy involves a complicated decision-making process involving comprehending risks associated with uncertain knowledge of potentially large numbers of complex, dynamically changing, uncontrollable (sometimes random and/or unknown/unknowable) factors.

Answering the question: “What is the risk of harming victim (i.e. non-target) systems (i.e., causing them to suffer degradation through interference)?” is complicated because of these complex issues. Addressing the question may be simplified by answering: “What is the risk of degradation to victim systems?” This naturally requires comprehending methods for probability calculation and coupling them to appropriate “consequence-metrics” with a relevant RA methodology. “Consequence-metrics” are quantified values for measuring the severity of a consequence, which could be (for example) percentage of system degradation in the context of EM equipment. This leads to the subsequent question: “What methods are available to calculate such probabilities and risks to victim systems?” Answering this question required a literature search for likely methods.

## III. SYSTEMATIC LITERATURE REVIEW

### A. Identifying mathematical methods

A systematic literature search using the SCOPUS database was performed to identify methods for the determination of victim probabilities and risks in IEMI. The first search focused on probability calculation methods; the second on RA methods utilising relevant consequence-metrics.

### B. Harm Probability methods

Filtration by review revealed eight potentially relevant probability calculation modelling methods based on ten references. These encompass Monte Carlo approaches, amongst others. This subset of methods and their associated references are summarised in Table I. The references (and ideas associated with each reference) were analysed against five ‘‘Problem Characterization Parameters’’ (5PCP). These 5PCP characterize the complicated nature of the IEMI context, namely: Scalability, Complexity, Dynamism, Uncertainty and Diversity. Regards dynamism, assessment of the references showed that those offering some evidence for how dynamism could be incorporated were Genender et al. [29], Liu Y. et al. [31] and the three by Peikert et al. [35] [36] [37]. Uncertainty and diversity required slightly more detailed evidential assessment which is summarised in Table I. Overall, only two references (Genender et al. and Peikert et al.) show evidence all 5PCP are addressed by their associated method. The philosophy behind their approaches was incorporated into the QRAM (see section IV).

TABLE I:  
POTENTIAL PROBABILITY METHODS  
MAPPING TO UNCERTAINTY AND  
DIVERSITY PCP

Reference	Uncertainty	Diversity
[11] Mao & Canavero	Maybe with an additional method	Hardware systems
[12] Genender et al	Yes. EMT with uncertainties	Anything using FTA
[13] Liu, Y. et al (2019)	Yes. Intended for use with uncertain/unknown parameters	Models Multi-State Components and Multi-State Systems
[14] Liu, Y. et al (2022)	Calculates confidence limits on Vulnerability PDFs	No Evidence
[15] Houret et al	Constraint calculation uses uncertain variables	Constraint & Susceptibility distributions only
[16] Sabath	No	Applies to EMI Threat Scenarios only
[17] Mondal et al	No	Could be applied outside of EMSO context
[18][19][20] 3 x Peikert et al	Yes. It uses Fuzzy-logic & set theory	Can diversify by increasing number and definition of fuzzy sets

### C. Risk Assessment methods

92 RA method references were individually reviewed leading to 18 potentially relevant RA method references listed in Tables II and III. Table II illustrates which of the references addresses consequence-metrics and Table III illustrates the type(s) of RA methodology covered within each paper. From a detailed analysis of all these

references, it was concluded that Li et al. [47] used a Monte Carlo type approach for assessing risk (and considers failure mechanisms exceeding thresholds) which would couple well with the approaches identified for probability calculations (in the previous subsection).

TABLE II  
POTENTIAL METHODS FOR DEFINING  
CONSEQUENCE METRICS

	Consequence Metric
[21] Liwang et al (2014)	Commanders to decide
[22] Paltrinieria et al (2019)	None
[23] Pasman et al (2017)	None
[24] Rawson et al (2021)	None
[25] Choi et al (2020)	Use MOE, MOP & MOCE with Attack Categories
[26] Devaraj et al (2021)	None
[27] Mansson et al (2009)	None
[28] Ruddle (2020)	Vectorised (Augmented) EMI Severity Classifications
[29] Devaraj, Ruddle, Duffy (2020)	None
[30] Li et al (2020)	Failure mechanisms exceeding thresholds
[31] Zhou et al (2018)	Interference Margins
[32] Xu et al (2023)	None
[33] Jang et al (2023)	Use MOE & MOP like Choi et al
[34] Butt & Jalil (2013)	Introduces jamming
[35] Howard & Stumptner (2005)	None
[36] Salnikova et al (2020)	None
[37] Sova et al (2020)	None
[38] Taherdoost, H. & Madanchian (2023)	None

TABLE III  
POTENTIAL METHODS FOR DEFINING THE  
RA METHOD

	RA - Graphical/BN	RA - Monte Carlo	RA - ML/DL	Non-Specific RA
[21] Liwang et al (2014)	No	No	No	No
[22] Paltrinieria et al (2019)	No	No	Yes	No
[23] Pasman et al (2017)	No	No	No	No
[24] Rawson et al (2021)	No	No	No	Yes
[25] Choi et al (2020)	No	No	No	No
[26] Devaraj et al (2021)	Yes	No	No	No
[27] Mansson et al (2009)	No	Yes	No	No
[28] Ruddle (2020)	No	No	No	No
[29] Devaraj, Ruddle, Duffy (2020)	Yes	No	No	No
[30] Li et al (2020)	Yes	Yes	No	No
[31] Zhou et al (2018)	No	No	No	No
[32] Xu et al (2023)	Yes	No	Yes	No
[33] Jang et al (2023)	No	No	No	No
[34] Butt & Jalil (2013)	No	No	No	No
[35] Howard & Stumptner (2005)	Yes	No	No	No
[36] Salnikova et al (2020)	No	No	Yes	No
[37] Sova et al (2020)	No	No	Yes	No
[38] Taherdoost, H. & Madanchian (2023)	No	No	No	Yes

#### IV. THE QRAM

##### A. The Approach

It is essential to recognise that the QRAM performs IEMI victim RA so (for instance) is not intended to replace EM test interactions with a mathematical model. Nor is it (in its current form) intended to evaluate EM equipment responses to high-level EM threats (although future work could develop it in this way). It is focused on the very real problem associated with Risk-Informed Decision-Making (RIDM) for transmitter operators in a battlefield scenario. To perform such victim RA the QRAM needs to model the victim equipment receiving a signal. The methods, revealed in the literature review, identified that the preferred RA approach is to model failure mechanisms exceeding thresholds, like the Li et al approach [30], thus leading to victim equipment degradation, but thresholds of what? As discussed earlier, detailed knowledge of victim system EM configurations is typically unknown/unknowable, however it is more likely that estimation of high-level equipment characteristics is possible. Such properties may be expressed in terms of parameters such as minimum input power, minimum Signal-to-Noise Ratio (SNR), antenna gain and saturation amongst other received-power-related values. There are also others related to received frequency, such as receiver min/max frequencies. The approach adopted is therefore based on the Li et al approach [30], modified to consider consequences beyond only component damage to model analysis of a simple front-door IEMI technique.

Estimating equipment parameters (and their potential distribution of possible values) is essential because calculating risk depends on estimating the probability that the received power and frequency causes some form of victim equipment degradation (occurring when the power/frequency exceeds equipment parameter thresholds). Referencing sources of data (e.g. experimental data for commercial equipment) to derive equipment parameters would be essential when constructing the equipment data for the QRAM input data, when applied to a real-life scenario. In addition to estimated equipment parameters, an essential element of the RA calculation is therefore to calculate the received power at the victim location, which must also account for the signal attenuation properties of the environment between transmitter and victim locations in addition to any intended received signal (i.e. in addition to the transmitter signal). This calculation is discussed in sub-section IV-B.

Of course, overlaying the requirements to calculate received power and model equipment parameters and victim location for the risk calculation, is the fact that there is a level of fuzzy

knowledge in the risk calculation because of the uncertainty in estimating equipment parameters and locations. This requires the use of estimated probability distributions representing the confidence and likelihood of a particular set of equipment parameters applying to a particular victim as well as the probability that a particular victim exists in a specific location. The necessity to model various model-features in a probabilistic way lends itself to the use of Monte Carlo for risk calculations. Such probability distributions can be sampled, and the received power/frequency used to determine if equipment thresholds are exceeded. So, for example, if a received power exceeds saturation (but for a saturation value that is selected randomly from a probability distribution of saturation values) then that is considered as causing degradation.

Sub-section IV-C discusses the use of probability distributions and the application of Monte Carlo in more detail. However, before proceeding with the details, an important feature of Monte Carlo calculations needs highlighting, which is that the method leads to only estimates of calculated values (in our case victim risk values). Such estimates (having used probability distributions to derive them) are themselves samples from a statistical distribution. This means several estimates must be obtained to calculate a mean value (in our case mean victim risk per victim), but also an estimate of the associated stochastic error (which is taken to be associated with the standard deviation of the mean).

The high-level activities involved in performing the QRAM are straightforward in the sense that they include the creation of input data, the execution of a python code and the visualization of power/risk (plus associated stochastic errors) distributions. There are a total of six input files including those containing the equipment parameters data, victim locations (and associated existence probabilities), signal direction data and material attenuation data relating to both the location of attenuation materials and the attenuation properties of those materials. In addition, there is a “Dashboard Data” file which contains a definition of the model geometry together with transmitter data and other runtime control data. The model geometry is based on a 3-dimensional cuboidal mesh with the number of orthogonal grid cells defined together with their relevant dimensions. Figure 1 shows an activity diagram summarizing the required high-level user actions with Figure 2 showing the flow and linkage of input data feeding into and out of the power calculation and into the QRAM. The green colored data boxes represent data from the “Dashboard Data”.

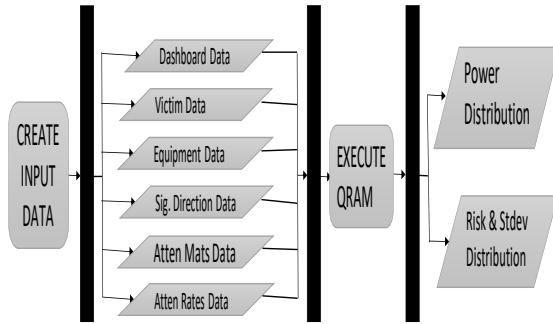


Figure 1: QRAM Activity Diagram

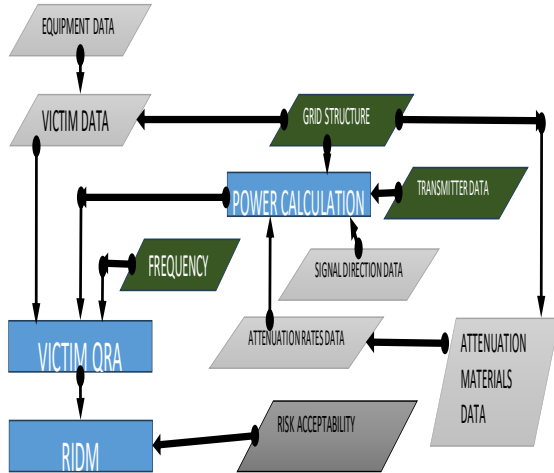


Figure 2: QRAM data flow diagram

### B. Calculation of received power

The calculation of received power requires knowledge of the power and mean frequency transmitted, the transmitter location and the victim location as well as the geometric and environmental attenuation properties of the intervening environment. Environmental attenuation is caused by buildings, vegetation and any other materials (gaseous, liquid or solid) whereas geometric attenuation is generally referred to as “Free Space Path Loss” (FSPL). For each grid cell the received power within it (in dBm) is first calculated using a FSPL model which is a straightforward calculation using transmitted frequency and involving the determination of the distance between the centre of each grid cell and transmitter grid cell. The environmental attenuation between these grid cell points is then estimated using a line-of-sight determination method that calculates stepwise attenuation values along that line by finding the attenuation material (from the user supplied attenuation materials map) at incremental points along the path and then utilising the user-supplied attenuation rate values associated with that material. Attenuation rate values define the reduction in dB per unit length (km) through an attenuation material (i.e. in units of dB/km). These are combined when the entire path between the central points of the

transmitter and grid cells has been traversed, so that it can be used to accordingly reduce the FSPL-determined received power leading to a determination of the transmitter-generated received power at the centre of each grid cell.

An assumption is that the received power values at these centre points apply across the whole associated grid cell. The accuracy of this assumption would depend on grid cell sizes chosen by the user. If sizes were large, then there may be significant variation of received power in the cell compared with the central value. However, this variation and its impact on the subsequent risk calculation is scenario dependent but could be estimated by users by reperforming calculations using different grid cell sizes to determine perturbation effects and hence potential systematic errors that may be associated with this approach.

In addition to transmitter power (which is an unintended received signal) there may also be intended signals for individual, specific victims, which are added to the unintended signal. These are user-supplied values for each victim system. The sum of the unintended and intended power values is then used in the subsequent determination of whether degradation occurs, and hence in the probability and risk calculations described next.

### C. Monte Carlo methodology and risk calculation

Details of the overall algorithmic process are described in this sub-section.

Each victim within each grid cell is assigned a unique integer (“the victim number”) within the user-defined victim data file, and each victim number is assigned an equipment number which aligns with a unique set of equipment parameters held within the equipment data file. The algorithm loops through each victim number to calculate its probability of degradation by using the assigned equipment parameters (in the form of mean values of a user-supplied associated probability distribution) and the algorithm then samples from each distribution to provide values of each required equipment parameter used in the Monte Carlo calculation comparisons.

This is repeated several times for each victim number; the number of times being equal to a user-defined number of “samples”. This sampling process leads to estimates of possible outcomes for each victim number based on its received power value. These outcomes could be degradation or not. A running tally of those samples causing degradation is kept for later use to calculate probability of degradation. The calculation then proceeds by looping through the number of user-defined samples in a user-defined set of batches.

For each individual sample, the algorithm first determines whether the victim can be affected by the

transmitted frequency or not. If not, then the sample is ended and the next sample is begun. Otherwise, the algorithm continues by next determining whether the minimum input power for the victim has been exceeded. This is where the pseudo code below begins. If not, then again, the sample is ended and the next sample is begun. Otherwise, the algorithm again continues by first increasing the received power by the equipment's antenna gain and then using that increased power to compare with the equipment saturation. If saturation is exceeded, then that sample is added to a tally of samples causing degradation for that victim number. If not, then the Signal-to-Intended-Noise Ratio (SINR) is compared with the equipment's minimum SNR (a randomly selected value of this) and if SINR is less than this value then the sample is added to the degradation tally. If not, then the sample ends and the next sample processed.

This algorithm and the specific equipment parameters used is usefully illustrated using pseudo code as shown below. Note in what follows, the values of the following four variables have been selected (prior to the algorithm described by the pseudo code) from user supplied probability distributions:

**min\_input** = minimum input power that the victim equipment can receive to function.

**gain** = antenna gain of victim equipment (dBm)

**saturation** = saturation of the victim equipment

**snr** = minimum SNR of victim equipment (dB)

In the pseudo code shown below the following variables are defined as described next:

**victim\_number** = An integer assigned to each victim (as described above)

**received\_power** = unintended signal due to the attacker's transmitter (discussed in IV-B)

**intended\_signal** = as discussed in IV-B

**gained\_victim\_power** = received power increased by antenna gain

**degradation\_band** = severity value of the consequence metric

**num\_bands** = number of different severity values of the consequence metric (in the cases run to date this =1)

**samples\_in[degradation\_band]** = array used to tally the number of samples causing degradation within each degradation\_band

**sinr** = Signal to Intended Noise Ratio (SINR). This is calculated for each victim number separately before the algorithm shown below.

In the pseudo code [39] that follows, commands are in capitals, variables in lower case and indentation used to align actions.

FOR EACH victim\_number:

IF (received\_power + intended\_signal) > min\_input THEN:

gained\_victim\_power = (received\_power + intended\_signal) + gain

IF gained\_victim\_power > saturation THEN:

degradation\_band = num\_bands  
samples\_in[degradation\_band] =  
samples\_in[degradation\_band] + 1

ELSE:

IF sinr < snr THEN:

degradation\_band =  
randomly selected from num\_bands  
samples\_in[degradation\_band] =  
samples\_in[degradation\_band] + 1

Once all samples in a batch for all victim numbers have been processed then the algorithm calculates the probability of degradation for that batch for each victim number by dividing the degradation tallies by the total number of samples in a batch. Victim risk for that batch for each victim number is then calculated by multiplying this probability by the consequence-metric. The metric in its simplest form is 100% degradation but the user can define consequence-metric bands if required and under those circumstances the tallies are determined and hence probabilities are calculated for individual consequence bands. The cases run to date use only 100% degradation or zero.

The probability of existence for each victim number is then determined from the user supplied existence probability values/distributions. The individual, calculated, victim risk values for an individual batch are then multiplied by their associated existence probability to determine modified victim risk values (for that batch) which account for the probability that each victim number exists in its associated grid cell.

At the end of each batch the victim risk distribution across the geometric grid is complete for the batch of samples. The value of calculated risk (for each victim number) is added to two tallies used to calculate mean risk values and standard deviations, as described next. Further batches are processed until all the user-defined batches are finished. By batching samples this enables a stochastic error on the calculated risk to be determined in the form of a standard deviation (as mentioned in IV-A). Recall, this stochastic error arises because the Monte Carlo calculation leads to merely estimates of risks from each batch. So, a set of estimates are gathered and a mean value for each victim is calculated along with its associated

standard deviation. Mean victim risk values for each victim number and associated standard deviations are calculated using the sum of victim risks for each victim number from each batch and the sum of squares of these victim risks. This is a standard approach to calculating mean and standard deviations [40]. The victim risk and standard deviations values (together with associated received power values) are output to a formatted data file that can be used to create visual illustrations of the power, risk and standard deviation distributions (examples of which are shown in the next section).

## V. VERIFICATION TESTING

### A. The Approach

There are many ways that an electromagnetic waveform can interact with a victim system. Exhaustive consideration of every possible type of interaction, with every possible class of victim system, would be prohibitively complex. Therefore, this paper has included the Li et al approach [30], to act as a reasonable representation of how the localised victim impact varies with the power of the EM signal at the victim. Future work may consider how to incorporate the wide range of possible interactions into this representation. QRAM validation (as opposed to verification) is thus not possible [41] because there is an infinity of scenarios each with associated dynamic, fuzzy knowledge (e.g. building attenuation properties). Validation would require a dedicated physical facility with known properties providing physically measured results with which calculated results could be compared. On the other hand, verification of the ontologically describable RA process [42] applied to RIDM is possible in the form of software assurance.

Assurance that software (like the QRAM) meets its requirements, and functional specification is thus achieved via verification testing which is a key task within typical Software Development Life Cycles like Waterfall [43] and V-Model [44]. For the QRAM, such testing is in three stages. Firstly (subsection V-B): tests to ensure that the power, risk and standard deviations distributions can be calculated along with changes to signal direction and attenuation materials. These are described here as “homogeneous tests”. Secondly (as explained in subsection V-C) tests ensure the variation of victim location distributions along with their existence probability leads to reasonable risk distributions. These are described as “heterogeneous tests”. The third stage (subsection V-D) demonstrates a state-of-the-art methodology assessment incorporating Systems-of-Systems (SoS) theory modelling which acts as a test to verify the QRAM with a (albeit fictitious) reasonably realistic scenario [41].

### B. Homogeneous Tests

These tests were performed using a geometrical grid of dimensions 1.1km x 1.1km x 1.0km and 11x11x1 cuboidal grid cells starting at (1,1,1) in the bottom left corner. The transmitter is in cell (6,6,1) emitting a power of 75dBm and a mean-frequency of 1GHz. This scenario is aiming to calculate effects over a large area and include the effect of receiver overload. Testing was performed through air-like materials with attenuation rates of 0, 2.5 and 5 (dB/km). The impact of increased attenuation was examined and found (as expected) to reduce the power distribution away from the transmitter towards the edges of the model.

The homogeneous tests were executed to determine victim risk distributions for a distribution of identical victim equipment with identical single-value existence probabilities of 25% because such output is relatively straightforward to verify given that such risk distributions will be symmetrical and decaying in value towards the geometry edges. Such tests also enable monitoring of the variation of standard deviations on the victim risk values to ensure that stochastic error values reduce appropriately with number of batches and sample sizes. Figure 3 shows the risk distribution for the case of 10,000 samples per batch and 100 batches. The associated standard deviation distribution is shown in Figure 4.

Further tests using non-zero attenuation rates within the geometry show the reduction in risk distribution towards the edges (e.g. see Figure 5 for 5 dB/km, 100 batches of 1000 samples per batch). The impact of varying existence probabilities was also tested to demonstrate that the risk distributions maintained their shape while the absolute values of risk varied linearly with existence probabilities as expected because (as mentioned toward the end of IV-C) these are simply multiplying factors. All cases were executed on a device with an i9-10885H CPU @ 2.40GHz. Runtimes demonstrated that execution takes ~3ms per Monte Carlo sample.

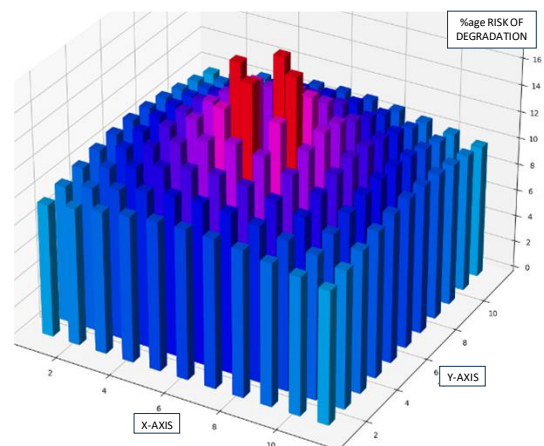


Figure 3: Example Risk distribution for homogenous tests

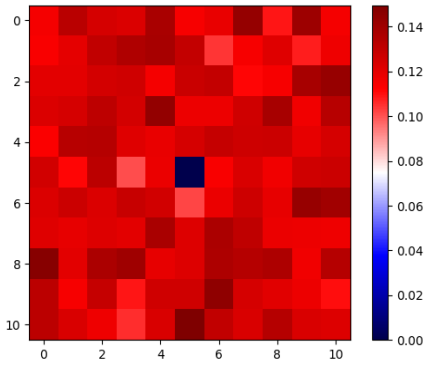


Figure 4: Example distribution of standard deviations for homogenous tests

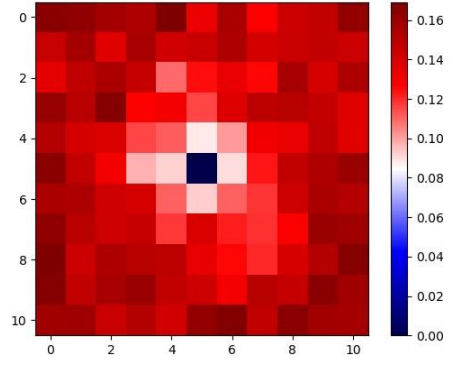


Figure 6: Example distribution of standard deviations for heterogeneous tests (for the risk distribution in Figure 8)

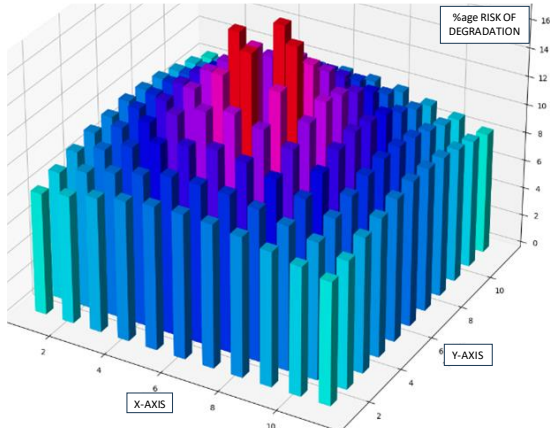


Figure 5: Example risk distribution for homogenous tests with attenuation rate 5 dBkm<sup>-1</sup>

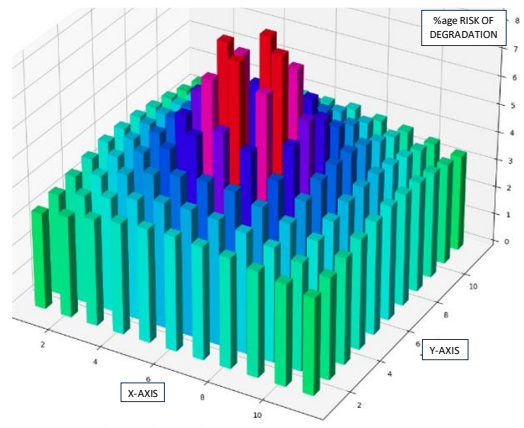


Figure 7: Example risk distribution for a victim with minimum SNR=8dB (Saturation=30dBm)

### C. Heterogeneous Tests

The heterogeneous tests were performed with individual grid cells containing more than one type of victim equipment (i.e. a heterogeneous spread), each having an existence probability of 10%, with the geometry grid being identical to the homogeneous tests. This enabled comparison of the impact of different equipment parameters on risk and standard deviations distributions for the transmission of the centralised 75dBm signal also used in the homogeneous tests grid. For instance, Figures 7 and 8 show an example of the impact on risk distribution of increasing the minimum SNR value for a victim such that increased probability of degradation (hence risk) occurs as expected because  $SINR < \text{Minimum SNR}$  which increases the number of samples causing degradation. This also reduces standard deviation values (see Figure 6). Further tests show the impact of varying victim equipment saturation and antenna gain values. For instance, risk reduces away from the central regions as saturation increases, as expected (compare Figure 8 with Figure 9).

Runtimes showed (as expected) an identical rate of ~3ms per Monte Carlo sample. This equated to a total runtime of 42 minutes for the case of 8 victims per cell which is a total of 960 victims in each heterogeneous model.

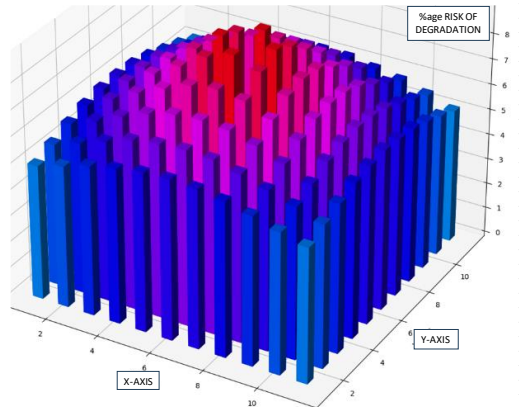


Figure 8: Example risk distribution for a victim with minimum SNR=20dB (Saturation=30dBm)

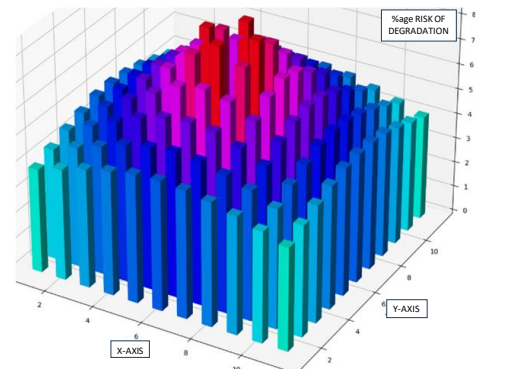


Figure 9: Example risk distribution for a victim with saturation=60dBm with minimum SNR=20dB

#### D. State-of-the-art Methodology Assessment Demonstration Test

Davies et al [41] applied the QRAM to a fictitious land-based scenario. The model details are given in Davies et al [41] so in the interests of brevity the following is a summary. There are four transmitter options, located at different geographical positions, in a suburban location. This contains habitable constructs (with their own associated estimated attenuation properties) each of which potentially contain various types of victim systems with various equipment properties. The location uncertainty is modelled using estimated “existence probabilities”. Estimates of statistically distributed potential victim equipment high-level parameters are incorporated. Risk calculations were performed for all four transmitter options leading to geographically distributed victim risk distributions demonstrating the application of the QRAM in an albeit relatively simple but realistic RIDM scenario.

#### VI. CONCLUSION AND FURTHER WORK

The term IEMI (defined in IEC 61000) is used throughout this article because the effects being considered are primarily impacting civilian infrastructure (the victims), as an indirect consequence of an intended military transmission. This article has focused only on that assessment of risk to victims, which is used in deciding whether to transmit or not. It is not focused on the assessment of risk in any other form. Validation and verification of the approach to risk assessment described in this article was discussed in section V.

In conclusion: this paper has described a novel QRAM capable of calculating IEMI scenario victim risk distributions in complex, dynamic, uncertain environments. Its novelty is the combination of methodologies, with an approach extending beyond merely physical aspects. The underlying methodology is founded on an extensive, initial systematic literature search using the SCOPUS database and a review of the identified literature which revealed potentially relevant mathematical modelling methods for performing IEMI victim RA. Whilst the systematic literature review outcomes revealed that existing IEMI QRAMs focus on only defender perspectives and apply to only relatively simple topologies, it was also recognised that a Monte Carlo type method adapted from ideas by Li et al [30] could be used as part of a victim RA in more complicated topologies together with similar approaches to those identified for probability calculations by Genender et al [12] and Peikert et al [18] [19] [20]. The development of the new QRAM was verified using significant sets of tests demonstrating that the QRAM developed to date provides a reasonable and useful tool for calculating first-order victim risk distributions with estimated stochastic errors which can be relatively easily

extended for more realistic IEMI scenarios by using suitably enhanced equipment data and attenuation data within more detailed user-described geometrical models. So, for instance, the QRAM utilises a database of EM equipment properties. This can be extended and enhanced (if required) by potential future users. This database is where the QRAM retrieves data enabling it to model such victim equipment properties as shielding and filtering (amongst other things). This novel approach of combining methodologies allows the generation of simple risk metrics that can be directly exploited by decision makers. The reliability of results from using the QRAM will depend on several factors. Firstly, the victim equipment data, the geometry (and attenuation) modelling of the environment and any directional-signal modelling will all have their own statistical modelling errors. Secondly, because this is a Monte Carlo method then there will also be stochastic errors. However, sensitivity analysis can be used (by running additional cases with revised data) to determine the impact of modelling errors, and stochastic errors can be minimised by simply running more calculations, increasing batch numbers or sample sizes.

Whilst the application examples described in section V are provided to show the verification of the QRAM, these examples are simply that: examples. The QRAM can be used in a variety of other ways to model for instance directional EM propagation where threat fields on target systems are focused, in the direction of the target.

Further work will develop an appropriate RIDM process which when automated and coupled with a relevant (and appropriately fast) QRAM will enable automated RIDM in complex, dynamic, uncertain environments like those in IEMI scenarios. Additional further work may examine Machine Learning methodologies (with suitable parallelisation) with a view to making the calculation runtimes of risk distributions faster, thereby potentially enabling real-time risk calculations to be performed.

#### VII. GLOSSARY OF ACRONYMS

EM: Electromagnetic  
 EMSO: Electromagnetic Spectrum Operations  
 ETA: Event Tree Analysis  
 FMEA: Failure Modes and Effects Analysis  
 FTA: Fault Tree Analysis  
 HAZOP: Hazard and Operability Studies  
 IEMI: Intentional Electromagnetic Interference  
 QRAM: Quantitative Risk Assessment Method  
 RA: Risk Assessment  
 RIDM: Risk-Informed Decision-Making  
 RM: Risk Management  
 SoS: Systems-of-Systems

## REFERENCES

- [1] HSE, 2013. *Managing for health and safety (HSG65)* [online]. Bootle, UK: HSE. Available from: <https://www.hse.gov.uk/pubns/books/hsg65.htm> [Accessed 29 January 2024].
- [2] Crawley, F. & Tyler, B., 2003. Hazard Identification Methods. Institute of Chemical Engineers, Rugby, Warwickshire.
- [3] BSI, 2016. *British Standard BS: IEC61882:2016 Hazard and operability studies (HAZOP studies) - Application Guide* [online]. Available from: <https://shop.bsigroup.com/ProductDetail/?pid=000000000030309555> [Accessed 29 January 2024].
- [4] IEC, 2018. *IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA)* [online]. Available from: <https://webstore.iec.ch/publication/26359> [Accessed 29 January 2024].
- [5] IEC, 2006. *IEC61025:2006 Fault tree analysis (FTA)* [online]. Available from: <https://webstore.iec.ch/publication/4311> [Accessed 29 January 2024].
- [6] IEC, 2010. *IEC 62502:2010 Analysis techniques for dependability - Event tree analysis (ETA)* [online]. Available from: <https://webstore.iec.ch/publication/7131> [Accessed 29 January 2024].
- [7] UK Civil Aviation Authority, 2023. *Introduction to bowtie* [online]. Available from: <https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/About-Bowtie/Introduction-to-bowtie/> [Accessed 29 January 2024].
- [8] ISO, 2018. *ISO31000:2018 Risk management — Guidelines* [online]. Available from: <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf> [Accessed 29 January 2024].
- [9] EMSOPEDIA, 2024. *Electro Magnetic Spectrum Operation* [online]. Available from: <https://www.emsopedia.org/entries/electro-magnetic-spectrum-operation-ems/> [Accessed 19 October 2024].
- [10] Radasky, W. A., Baum, C. A. and M. W. Wik, 2004. Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI), *IEEE Transactions on Electromagnetic Compatibility*, 46 (3), 314-321.
- [11] Mao, C. & Canavero, F., 2016. System-Level Vulnerability Assessment for EME: From Fault Tree Analysis to Bayesian Networks -Part I: Methodology Framework. *IEEE Transactions on Electromagnetic Compatibility*, 58(1), 180-187, 7317576.
- [12] Genender, E., Garbe, H. & Sabath, F., 2014. Probabilistic risk analysis technique of intentional electromagnetic interference at system level. *IEEE Transactions on Electromagnetic Compatibility*, 56(1), 200-207, 6568885.
- [13] Liu, Y., Han, F., Wang, J. & Qi, H., 2019. Vulnerability assessment of a multistate component for IEMI based on a Bayesian method. *IEEE Transactions on Electromagnetic Compatibility*, 61(2), 467-475, 8353367.
- [14] Liu, Y., Du, P., Han, F., Xia, H. & Wang, J., 2022. A Bayesian Estimation of Confidence Limits for Multi-state System Vulnerability Assessment With IEMI. *IEEE Transactions on Electromagnetic Compatibility*, 64(4), 1219-1229.
- [15] Houret, T., Besnier, P., Vauchamp, S. & Pouliguen, P., 2020. Probability of Failure Using the Kriging -Controlled Stratification Method and Statistical Inference. *Proceedings of the 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE, EMC EUROPE 2020*, 9245860.
- [16] Sabath, F., 2014. EMI risk management with the threat scenario, effect, and criticality analysis. *Ultra-Wideband, Short-Pulse Electromagnetics*, 10, 265-278.
- [17] Mondal S. K., Tan, T., Khanam, S., Kabir, H. M. D. & Ni, K., 2023. Security Quantification of Container-Technology-Driven E-Government Systems. *Electronics*, 12, 1238.
- [18] Peikert, T., Garbe, H. & Potthast, S., 2015. A fuzzy approach for IEMI risk analysis of IT-Systems with respect to transient disturbances. *IEEE International Symposium on Electromagnetic Compatibility*, 1077-1082, 7256318.
- [19] Peikert, T., Garbe, H. & Potthast, S., 2016. Risk analysis with a fuzzy-logic approach of a complex installation. *Advances in Radio Science*, 14, 91-96.
- [20] Peikert, T., Garbe, H. & Potthast, S., 2017. Fuzzy-Based Risk Analysis for IT-Systems and Their Infrastructure. *IEEE Transactions on Electromagnetic Compatibility*, 59(4), 1294-1301, 7892009.
- [21] Liwang, H., Ericson, M. & Bang, M., 2014. An examination of the implementation of risk-based approaches in military operations. *Journal of Military Studies*, 5(2).
- [22] Paltrinieria, N., Comfort, L. & Reneirs, G., 2019. Learning about risk: Machine learning for risk assessment. *Safety Science* 118, 475-486.
- [23] Pasman, J., Rogers, W. J. & Mannan, M. S., 2017. Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Safety Science* 99, 140-155.
- [24] Rawson, A., Brito, M., Sabeur, Z. & Tran-Thanh, L., 2021. From Conventional to Machine Learning Methods for Maritime Risk Assessment. *International Journal on Marine Navigation and Safety of Sea Transportation*, 15 (4), 757-764.
- [25] Choi, S., Kwon, O.-J., Oh, H. & Shin, D., 2020. Method for effectiveness assessment of electronic warfare systems in cyberspace. *Symmetry*, 12(12), 1-16, 2107.
- [26] Devaraj, L., Ruddle, A.R. & Duffy, A.P., 2021. EMI Risk Estimation for System-Level Functions Using Probabilistic Graphical Models. *Joint IEEE International Symposium on Electromagnetic Compatibility Signal and Power Integrity, and EMC Europe, EMC/SI/PI/EMC Europe 2021*, 851-856.
- [27] Mansson, D., Thottappillil, R. & Backstrom, M., 2009. Methodology for classifying facilities with respect to intentional EMI, *IEEE Transactions on Electromagnetic Compatibility*, 51 (1), 46-52.
- [28] Ruddle, A. R., 2020. Risk Analysis for Automotive EMC: Scope, Approaches and Challenges, *Proceedings of the 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, 9245774.
- [29] Devaraj, L., Ruddle, A.R. & Duffy, A.P., 2020. System Level Risk Analysis for Immunity in Automotive Functional Safety Analyses, *Proceedings of the 2020 International*

- Symposium on Electromagnetic Compatibility - EMC EUROPE*, 9245692.
- [30] Li, K.-J., Xie, Y.-Z., Chen, Y.-H., Zhou, Y. & Hui, Y.-C., 2020. Bayesian inference for susceptibility of electronics to transient electromagnetic disturbances with failure mechanism consideration, *IEEE Transactions on Electromagnetic Compatibility*, 62 (5), 1669-1677.
- [31] Zhou, P., Lv, Y., Chen, Z. & Xu, H., 2018. System-level EMC assessment for military vehicular communication systems based on a modified four-level assessment model, *China Communications*, 15(8), 39–53, 8438272.
- [32] Xu, T., Chen, Y., Wang, Y., Zhang, D. & Zhao, M., 2023. EMI Threat Assessment of UAV Data Link Based on Multi-Task CNN, *Electronics* (Switzerland), 12(7), 1631.
- [33] Jang, J., Kim, K., Yoon, S., Ahn, M. & Shin, D., 2023. Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated with Cyber Asset Damage, *IEEE Access*, 11, 45113–45128.
- [34] Butt, F.A. & Jalil, M., 2013. An overview of electronic warfare in radar systems, *The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering*, 213–217, 6557273.
- [35] Howard, C. & Stumptner, M., 2005. Probabilistic reasoning techniques for situation assessments. *Proceedings - 3rd International Conference on Information Technology and Applications*, 383–386, 1488832.
- [36] Salnikova, O., Cherviakov, O., Sova, O., ...Neroznak, Y., & Proshchyn, I., 2020. Development of an improved method for finding a solution for neuro-fuzzy expert systems. *Eastern-European Journal of Enterprise Technologies*, 5(4-107), 35–44.
- [37] Sova, O., Shyshatskyi, A., Malitskyi, D., ...Shevchuk, V. & Sova, M., 2020. Development of a complex method for finding a solution for neuro-fuzzy expert systems. *Eastern-European Journal of Enterprise Technologies*, 6(4-108), 22–31.
- [38] Taherdoost, H. & Madanchian, M., 2023. Multi-Criteria Decision Making (MCDM) Methods and Concepts, *Encyclopedia*, 3(1), 77-87.
- [39] Dalbey, J., 2003. *Pseudocode Standard*, [online]. Available from: [https://users.csc.calpoly.edu/~jdalbey/SWE/pdl\\_std.html](https://users.csc.calpoly.edu/~jdalbey/SWE/pdl_std.html) [Accessed 25 October 2024].
- [40] BBC, 2024. *Bitesize. Standard Deviation. The formulae.*, [online]. Available from: <https://www.bbc.co.uk/bitesize/guides/zcqv4wx/revision/2> [Accessed 25 October 2024].
- [41] Davies, N., Dogan, H. & Ki-Aries, D., 2025. Application of Systems-of-Systems Theory to Electromagnetic Warfare Intentional Electromagnetic Interference Risk Assessment., *Systems*, 13 (4), 244.
- [42] Davies, N., Dogan, H., Ki-Aries, D., Jiang, N. & Williams, C., 2024. Foundations for Modelling Conscientious Attacking in Electromagnetic Cyberspace, *IEEE International Conference on Cyber Security and Resilience (CSR)*, London, United Kingdom, 2024, 726-731.
- [43] Royce, W. W., 1987. Managing the Development of Large Software Systems, *Proc. 9th. Intern. Conf. Software Engineering*, IEEE Computer Society, 328-338 (Originally published in Proc. WESCON, 1970).
- [44] Forsberg, K. & Mooz, H., 1991. The Relationship of System Engineering to the Project Cycle, *Proc. First Annual Symposium of National Council on System Engineering, October 1991*, 57–65.