systems

MDPI

Article

Application of Systems-of-Systems Theory to Electromagnetic Warfare Intentional Electromagnetic Interference Risk Assessment

Nigel Davies *, Huseyin Dogan and Duncan Ki-Aries

Faculty of Science & Technology, Bournemouth University, Poole BH12 5BB, UK; hdogan@bournemouth.ac.uk (H.D.); dkiaries@bournemouth.ac.uk (D.K.-A.)
* Correspondence: ndavies2@bournemouth.ac.uk

Abstract: Battlefields contain complex networks of electromagnetic (EM) systems, owned by adversary/allied military forces and civilians, communicating intentionally or unintentionally. Attacker's strategies may include Intentional EM Interference (IEMI) to adversary target systems, although transmitted signals may additionally degrade/disrupt allied/civilian systems (called victims). To aid decision-making processes relating to IEMI attacks, Risk Assessment (RA) is performed to determine whether interference risks to allied/civilian systems are acceptable. Currently, there is no formalized Quantitative RA Method (QRAM) capable of calculating victim risk distributions, so a novel approach is proposed to address this knowledge gap, utilizing an Electromagnetic Warfare (EW) IEMI RA method modeling scenarios consisting of interacting EM systems within complex, dynamic, diverse, and uncertain environments, using Systems-of-Systems (SoS) theory. This paper aims to address this knowledge gap via critical analysis utilizing a case study which demonstrates the use of an Acknowledged SoS-based model as input to a QRAM capable of calculating victim risk distributions within EW IEMI RA-associated scenarios. Transmitter operators possess only uncertain/fuzzy knowledge of victim systems, so it is proposed that a Moot Acknowledged System-of-Fuzzy-Systems applies to EW IEMI RA scenarios. In summary, a novel SoS description feeding a novel QRAM (supported by a systematic literature review of RA mathematical modeling techniques)is proposed to address the knowledge gap.

Keywords: electromagnetic warfare; electromagnetic interference; risk assessment; risk acceptability; systems-of-systems

Academic Editors: Michael Henshaw, Ed Pohl and Siyuan Ji

Received: 13 December 2024
Revised: 6 February 2025
Accepted: 31 March 2025
Published: 1 April 2025

Citation: Davies, N.; Dogan, H.; Ki-Aries, D. Application of Systems-of-Systems Theory to Electromagnetic Warfare Intentional Electromagnetic Interference Risk Assessment. *Systems* **2025**, *13*, 244. https://doi.org/10.3390/systems13040244

1. Introduction

Knowledge of the whereabouts of enemy forces and allied forces is essential for "Command and Control" in warfare, which relies on communications systems for observation of battlefield operations. Primarily, such communications use electromagnetic (EM) radiation using EM systems, e.g., RADAR or LIDAR, which are active systems transmitting EM signals and utilizing sensors for the detection of reflected signals, and are typically used for air-defense, aviation, and artillery. However, there are also passive systems that purely collect EM signals for gathering "signals intelligence" (SIGINT) from adversary sources such as radios, RADAR, or heat (from people, missiles, aircraft, artillery, vehicles, etcetera). In addition, some systems are used for electromagnetically attacking targets (i.e., adversary EM systems), by transmitting EM signals intentionally with the specific objective of degrading or disrupting target systems. Such signal transmission aimed at inflicting interference on target systems is called Intentional EM Interference (IEMI) [1–3],

but problems arise because the transmitted signals may additionally degrade or disrupt allied or civilian systems (called victim systems). Civilian systems within a battlefield may (for example) belong to hospitals, schools, commercial businesses, infrastructure facilities, domestic premises, etcetera. There may also be intercommunications from/to such civilian systems that may be impacted. A battlefield is therefore a set of EM systems that are all either communicating intentionally or unintentionally, forming a complex network of systems. Attempting IEMI is thus technically complicated because optimal decisions on emitted signal frequency/power require knowledge of target architecture (knowledge often unknown/unknowable). The architecture comprises many varied EM components formed into many electromagnetically interacting sub-systems (i.e., EM devices are Systems-of-Systems (SoS)) [4]. It is further complicated by target location uncertainty and complex EM environment topologies. Additionally, victims also have associated architecture/location uncertainties. Therefore, determining the appropriate IEMI target-focused 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, all potentially associated with a System of SoS.

To aid military commanders in the decision-making process relating to IEMI attacks and the signal transmission strategy to adopt, a Risk Assessment (RA) is often performed for such operations to determine whether interference to allied/civilian systems is an acceptable risk or not, because victim interference may (or may not) benefit the attacker (depending on the attacker's risk appetite). In other words, RA within a System of SoS is required to determine whether interference risks to allied/civilian systems are acceptable; however, currently, there is no formalized Quantitative Risk Assessment Method (QRAM) to perform this, so a novel approach is required to address this knowledge gap.

A formalized, Electromagnetic Warfare (EW) IEMI QRAM and the associated scenarios assessed consist of interacting systems of EM systems. However, do they form a strictly defined SoS? If so, then what type of SoS? This paper aims to address these questions and the identified knowledge gap with the objective of demonstrating a QRAM used for calculating victim risk distributions for a case study using a geometrical SoS-based model. In summary, the aim is to use a case study to demonstrate that SoS theory can be applied in an EW IEMI QRAM.

Section 2 describes a systematic literature review of RA mathematical modeling techniques used to determine principal methods for performing the EW IEMI RA within an SoS-based model. Section 3 describes the methodology covering the details of the QRAM, as well as the case study-based approach adopted for demonstrating the overall methodology. Section 4 describes the case study scenario and a background to the data and SoS elements, together with the results from the QRAM. Section 5 provides a discussion around the relevance to SoS, EW IEMI operations, and the development of the use of the proposed QRAM. Section 6 concludes, including ideas for further work.

2. Literature Review: EW IEMI RA and SoS

2.1. Electromagnetic Spectrum Operations and EW

Electromagnetic Spectrum Operations (EMSO) provides data/information essential in warfare and other military operations like peacekeeping. It is defined as

> *"Military actions to exploit, attack, protect, and manage the electromagnetic operating environment".* [5]

These are complex operations involving military personnel and EM systems [6,7] and the functionality of such systems can be interfered with by adversaries in conventional ways but also using electromagnetic (EM) signals instead which cause EM interference.

During EW, preventing an adversary's EM equipment (i.e., radio communications devices) from fully functioning is beneficial to opponents. Often, in military operations, attempts to cause interference in EM equipment are intentional (i.e., IEMI). However, attempts at IEMI cannot guarantee interference of target systems because EM interference relies upon factors such as successfully penetrating shielding technologies and attaining directionally correct, sufficient power at appropriate signal frequencies. 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, thereby causing potentially indeterminate system effects. So, attempting IEMI is technically complicated because optimal decisions on emitted signal frequency/power require knowledge of the target architecture (which is often unknown/unknowable). Target architectures comprise many varied EM components formed into many electromagnetically interacting sub-systems (i.e., EM equipment form an SoS) [4].

Hazard Identification and Analysis methods, e.g., [8–10], such as Hazard and Operability Studies (HAZOP) [11], Failure Modes and Effects Analysis (FMEA) [12], Fault Tree Analysis (FTA) [13], Event Tree Analysis (ETA) [14], and Bow-Tie Analysis [15], are often used in Safety Risk Management (with sufficient knowledge) to model EM systems to aid analysis of victim system interference, although from a Safety Risk Management perspective the primary aim of such methods is avoidance of damage (from hazards). However, in EW IEMI scenarios an attacker is targeting a potentially unknown (and/or unknowable) target structure in an unknown (and/or unknowable) state while simultaneously considering the risk of interference to victims (with a similar level of uncertain knowledge). EM systems within a battlefield used in EMSO are therefore only fuzzily defined.

2.2. Applicability of SoS to EW IEMI RA and Critical Analysis of SoS Types

The definition of SoS is

> *"A set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish independently. Note 1 to entry: Systems elements can be necessary to facilitate the interaction of the constituent systems in the systems of systems".* [16]

However, is there a "unique capability" associated with EW IEMI RA scenarios?

The concept of "Resilience" can provide a method of answering the question above, by first tackling the following: "How does 'Resilience' relate to EW IEMI RA scenarios"?

There are three dimensions to "Resilience" (performance, characteristics, and structure) [17]. Performance is difficult to conceptualize in EW IEMI RA scenarios other than the performance (by the attacking military commanders) of some form of QRAM. Let us examine EW IEMI RA scenarios in more detail to assess this. A scenario can be defined by a set of varied information that can be written as follows:

$$\{B, S, C, V, L, G, M, W\}$$

where

B = Battlefield
S = Source location
C = Communications and Consultations (C&C) with victims
V = Victim equipment types
L = Location of victims
G = Geophysical and geographical features

M = Meteorology (inc. solar and brightness)
W = Wildlife (e.g., birds)

All this information can be collected in a data table (illustrated in Figure 1), which indicates there could be an infinity of scenarios.

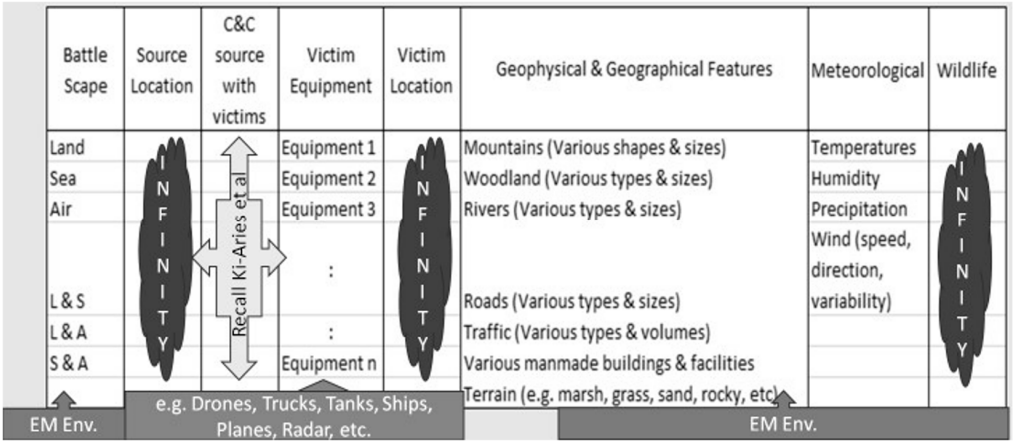

Figure 1. Scenario information.

To conceptualize "performance" (and what weakened performance might mean) in EW IEMI RA scenarios involves performing some type of Verification and Validation (V&V) on any modeling method utilizing an EW IEMI RA scenario. So, performance is simply the ability to calculate victim risks for a given scenario, i.e., to perform a QRAM.

This discussion on the concept of "performance" for the SoS applying to the specific context of EW IEMI RA scenarios is aided by the concept of "SoS mission". Olivero et al. [18] make some important observations on this:

- *"The attractiveness of SoS architectures descends from the fact that the SoS collective behavior can achieve goals that would be infeasible by having the constituent systems working in isolation".*
- *"In the literature such collective goals are referred to as the SoS missions".*

An immediate observation is that an EW IEMI RA scenario has no mission, unless the mission is simply to perform a RA. But as Olivero et al. [18] further observes:

- *"Explicitly identifying and modelling a SoS mission may provide key guidance for SoS design and validation".*
- *"A mission conceptual model can help in representing and relating the main elements of the SoS emergent behavior"*

Olivero et al. also note the non-functional properties of SoS missions by referring to previous studies. For example, Silva et al. [19] proposed mKAOS, a mission-oriented language and approach for modeling and designing SoS, whereas Chiprianov et al. [20] concluded that SoS mission success may be affected by poor resulting global performance, security, or other non-functional properties (NFPs). What Olivero et al. conclude is that modeling and addressing SoS NFPs is "largely unexplored" by observing SoS NFPs, which are "*hardly measurable or predictable in a SoS, due to their uncertain and dynamic nature*".

So, while these are important considerations for an SoS with a mission, in EW IEMI "a mission" (for the transmitter operator, or a target operator, or a victim system operator, etcetera) is not an "SoS Mission" but is the mission of a specific constituent part of the SoS. In EW IEMI RA, the transmitter operator command chain has a mission to perform RA to decide whether to transmit a signal of a given power and frequency, but that is not the mission of the SoS as a whole. The mission (in using this SoS) is to provide a model for performing a very specific RA for calculating a very specific type of risk, i.e., calculating risk to a variety of

individual victim systems. The type of "mission" discussed by Olivero et al. [18] is not this type of mission. However, the EW IEMI RA scenario "Mission" could be simply "to perform RA capable of calculating victim risk distributions" which is a "unique capability" sufficient to justify the assumption that SoS theory can be applied and enables an assessment of the type of SoS that might apply to an EW IEMI RA scenario.

Recall there are four SoS types [21]:

- Directed: built and managed to fulfil specific purposes;
- Acknowledged: recognized objectives, and designated management and resources (but constituent systems retain independence);
- Collaborative: no central management with coercive power—elements collaborate voluntarily;
- Virtual: no central management or purposes. Exists deliberately or accidentally (SoS behavior emerges, via informal elemental collaboration & individual element management).

"Directed" can be dismissed here on the basis that an EW IEMI RA scenario is certainly not "built" in the normal sense of the word. Its construction is an ad hoc conglomeration of whatever EM systems happen to be in the geographical area at the time the transmitter operator has chosen to be sited in its location. These can be fixed facilities (i.e., schools, hospitals, etcetera) or mobile ones (e.g., mobile civilian, allied, or adversary systems). However, there is no overall SoS manager who has designed and built the scenario to fulfil some specific purpose. So, an applicable SoS is not "Directed".

"Collaborative" can similarly be dismissed because there is certainly no obvious overall collaboration. There are interactions and some elements within the scenario may (or may not) collaborate voluntarily. The attacker controlling the transmitter may (or may not) collaborate with allied forces. They may (or may not) interact with owners of other victim systems; however, it is unlikely they will collaborate with a target system owner. So, whilst parts of a scenario's constituents may be involved in some form of collaboration, certainly others will not be; therefore, an applicable SoS is not "Collaborative".

Given the description of an "Acknowledged" SoS and the above discussion implying potentially a lack of recognized objectives, plus the points made above regards a lack of management, it appears to be relatively straightforward to dismiss "Acknowledged" SoS. However, let us examine these points in detail. Firstly, the reason why there is this discussion on SoS types is because we could assume that the recognized objective is "to perform RA capable of calculating victim risk distributions". Secondly, assuming the objective holds true, there is a "designated manager" for performing "RA capable of calculating victim risk distributions", who is clearly the decision-maker (i.e., the attacking transmitter controller). Thirdly, there are recognized resources in the scenario, albeit there may be uncertainty associated with resource existence, location (if existing), equipment specification/purpose, etcetera, while noting constituent systems retain independence. So, an "Acknowledged" SoS is potentially applicable (depending on how the word "objectives" is defined).

Finally, it is tempting, prima facie, to highlight "Virtual" as the most applicable SoS, because if there is no central management or purpose (i.e., no mission, no objective) as discussed above, then it fits the description. Further, the point has been made that whilst an EW IEMI RA scenario could exist deliberately it is more likely to be ad hoc (perhaps it exists accidentally?). Furthermore, it is easy to imagine that, within such an SoS, informal elemental collaboration occurs. However, if an attacker can decide to impact a victim system there is an argument that individual element management is not maintained, because an attacker may be able to control one or more victim systems. This implies a level of management within a scenario. It is also not obvious how emergent behavior is observed because emergent behavior of such an SoS is not visible to all elements in such an

SoS. Even the attacker cannot measure (with certainty) the emergent behaviors within an EW IEMI RA scenario.

The above critical analysis of the four main types of SoS concludes that the type of SoS that applies to EW IEMI RA is an Acknowledged SoS. Figure 2 illustrates how this model fits source and victim equipment aspects of the EW IEMI RA scenario information shown in Figure 1.

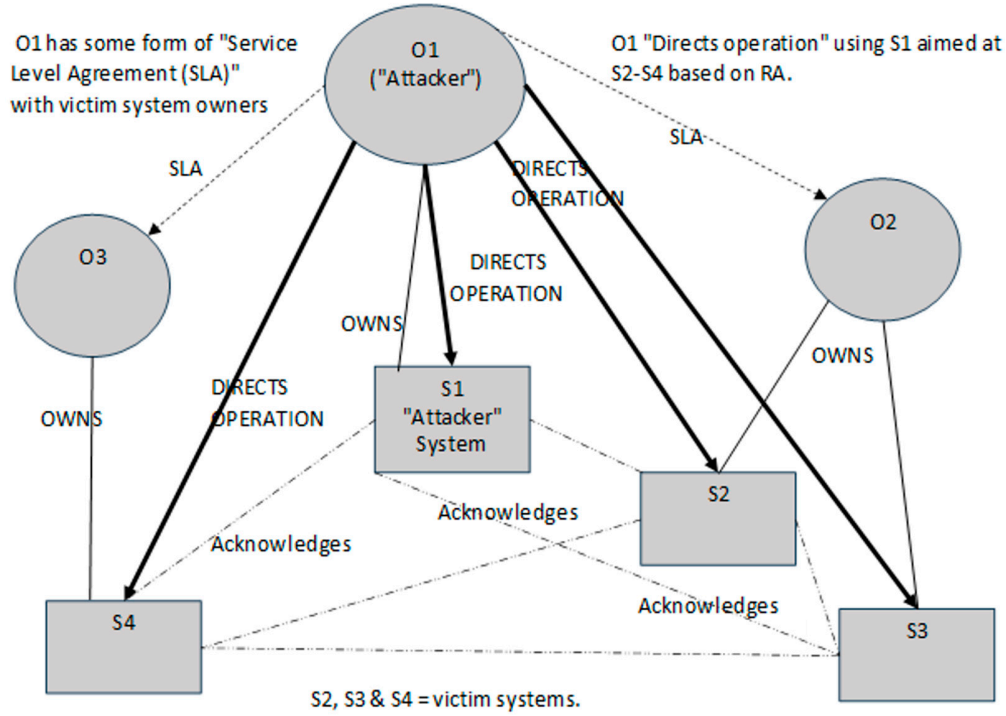

Figure 2. Type of SoS that EW IEMI RA applies to (adapted from Dahmann [22]).

Some of the terminology used by Dahmann [22] in Figure 2 does not fit easily into EW IEMI RA scenarios. Further, the target system (and its controller O(E)) should be added. So, Figure 2 was modified (see Figure 3).

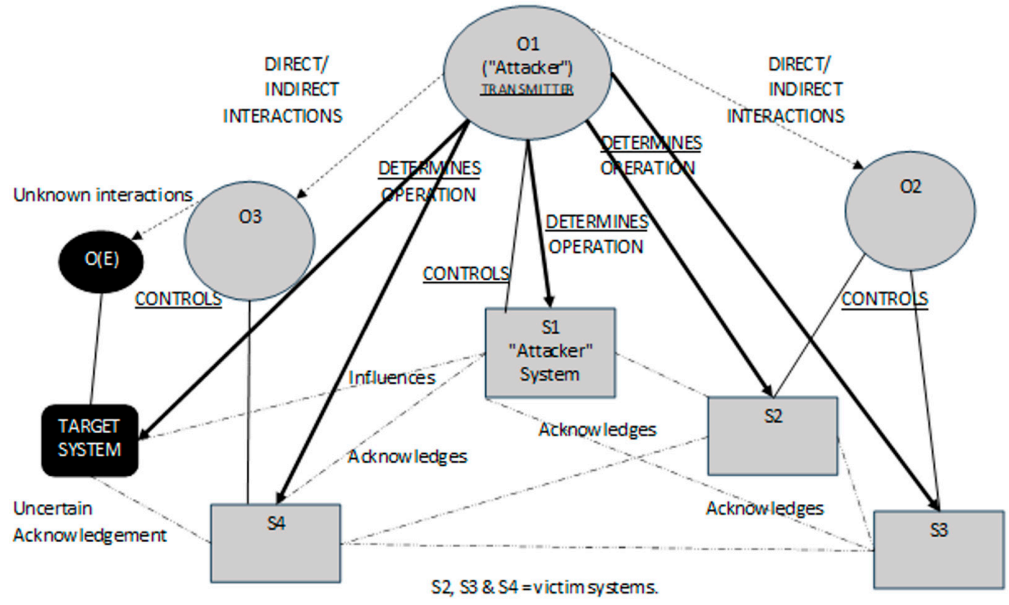

Figure 3. Acknowledged SoS for EW IEMI RA (adapted from Dahmann [22]).

Figure 3 illustrates the SoS boundaries, and anything outside those is not part of what is being considered in this scenario. Observe in Figure 3 that there are various direct/indirect interactions. Such interactions are like those found in ecological communities. and a deeper examination of these (e.g., by Moon et al. [23]) indicates there are different types of direct/indirect interactions. In this Acknowledged SoS (between, e.g., "O1 and O2" or "O1 and O3") these interactions are in reality "Human Interactions" (HIs) where communication between people is performed (in whatever form) to gain information. The motivation may be (for instance) to determine the level of trust between the two people. However, in EW IEMI there is unlikely to be communications between "O1 and O(E)" although, by virtue of O1 controlling the signal propagating from S1, O1 can determine the operation of O(E). There may also be system acknowledgement between other systems (e.g., S4) and the target system; however, this communication is not known to O1 and may be known to only a subset of operators in the SoS.

2.3. Harm Identification and Risk Assessment

A systematic literature search used the SCOPUS database to identify a selection of methods (in published research to date) usable for the determination of victim probabilities and risks in IEMI. It involved two phases of literature search: one focused on relevant probability calculation methods and the other on relevant RA methods utilizing relevant consequence metrics. The review utilized guidance by Xiao and Watson [24] and referred to guidance from PRISMA [25], Fourie [26], Shukla et al. [27], and others [28–34] (Figure 4 illustrates the process).

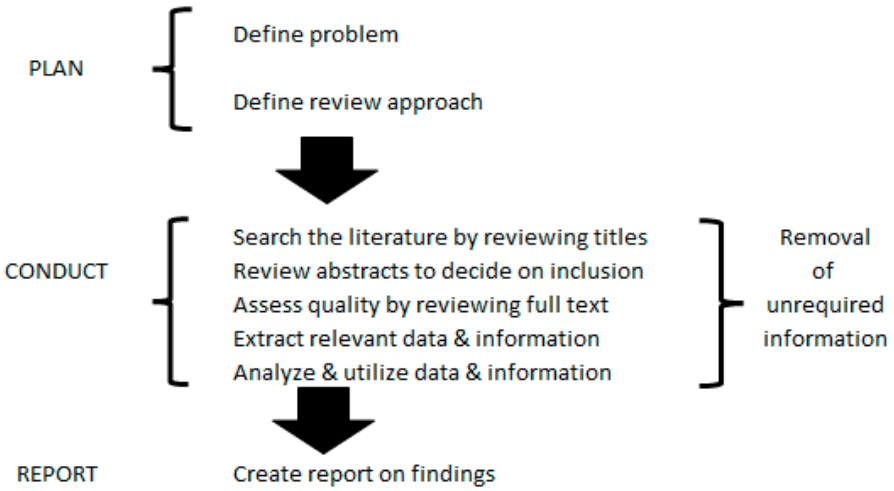

Figure 4. Systematic literature review process.

A broad taxonomy of 29 thematic clusters for 229 probability methods references was manually created and used to select methods for the analysis of IEMI risks. The review revealed 8 potentially relevant mathematical modeling methods based on 10 references within the "Methods Improvement" thematic cluster [35–44]. These encompass Monte Carlo approaches, Bayesian techniques, Statistical Inference, and the use of Fuzzy Logic-related conditioned data. The 92 RA method references were all individually reviewed, leading to 18 potentially useful references [45–62].

3. Methodology

3.1. Description of the QRAM

The literature revealed the preferred QRAM approach to modeling EM systems degradation was to model failure mechanisms exceeding thresholds. Due to detailed knowledge

of victim system EM configurations being unknown/unknowable, the application of this approach to high-level equipment characteristics and parameters is possible. Adopting this approach additionally requires estimation of the received power/frequency at the victim location, accounting for the topology between transmitter and victim locations. These various model features needed to be modeled in a probabilistic way due to the uncertainties associated with them, and this lends itself to the use of Monte Carlo. Sampling of distributions is based on the received power/frequency to determine if thresholds are exceeded. Details on the QRAM methodology are described by Davies et al. in a paper specifically focused on the detailed QRAM and its verification [63].

The calculated risk associated with each consequence is derived from the QRAM, which in this context is constructed based on the methodology discussed and defined by "The Spectrum and Receiver Performance Working Group of the Federal Communications Commission's (FCC) Technological Advisory Council" [64] in 2015 on "Risk Informed Interference Assessment" (RIIA) (see Figure 5). The QRAM calculates the risk of degrading a victim system, which depends on the power and frequency transmitted, the location of the transmitter and victim, several victim system characteristics, environmental characteristics capable of attenuating EM signals (usually described as EM topology), and probabilistic factors that model the uncertainty of victim system characteristics and location. The QRAM therefore provides a set of risk values (in11qq of percentage degradation) for each separate, individual victim system.

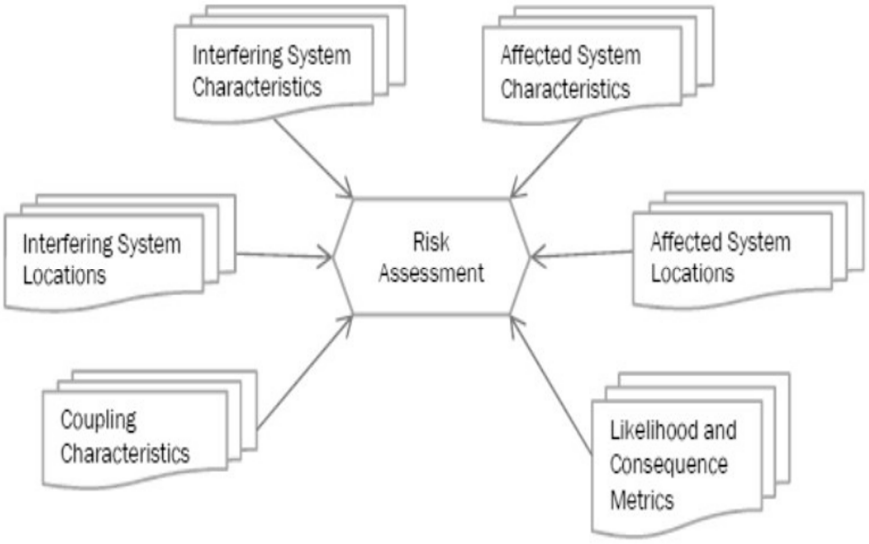

Figure 5. Risk-informed interference assessment (replicated from De Vries [64]).

3.2. Case Study Based Approach for the Critical Analysis of the Proposed SoS Type

It was concluded in Section 2.2 that EW IEMI RA scenarios are SoS. Further, based on the high level of uncertainty of knowledge of attacking transmitter operators (which implies that the constituent systems are fuzzily defined), it was proposed that an Acknowledged SoS that nevertheless does not necessarily have well defined elements applies to EW IEMI RA scenarios. But how can such a proposal be critically analyzed?

The approach adopted here is to use a model of an EW IEMI RA scenario encompassing a typical set of complex, dynamic, diverse, and uncertain environmental features while incorporating an Acknowledged SoS to aid modeling the associated EM topology. The objective is to demonstrate that a QRAM process can be performed to calculate victim risk distributions using this SoS model. This provides a case study that can be critically analyzed to assess what advantages and disadvantages the Acknowledged SoS-based model provides.

4. Case Study: EW IEMI QRAM Using an SoS-Derived Model

4.1. Description of the Scenario

The methodology described above was tested using a fictitious land-based EW IEMI scenario. In this scenario, a commander needs to degrade a transmitter located on a farm. The commander knows the frequency bandwidth to transmit at but is not sure of (i) power to transmit, (ii) transmitting equipment, or (iii) best location. Due to operational reasons and the requirements for ensuring that target system interference was potentially achievable, there are four differing transmitter power values and locations. Option 1 used 25 dBm, Option 2 used 50 dBm, Option 3 used 75 dBm, and Option 4 used 100 dBm. The question the scenario aims to address is the following: What are the victim risk distributions for each transmission signal and location option? Figure 6 illustrates a two-dimensional map of the geographical layout of the village near the target location.

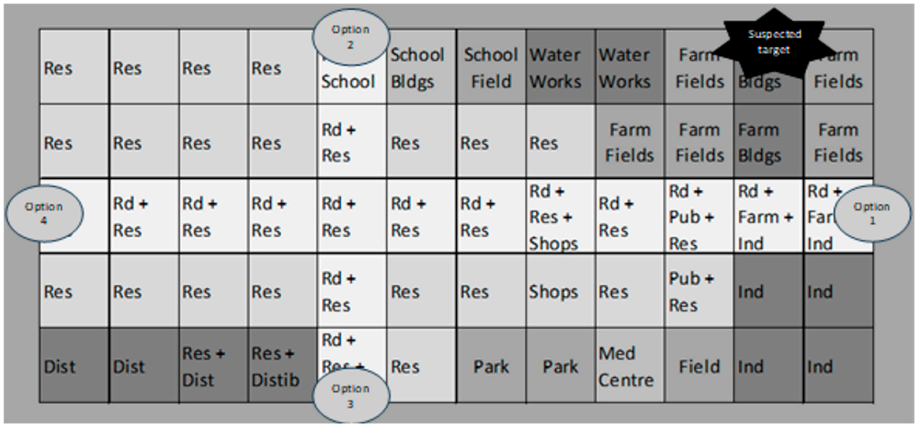

Figure 6. Map of the fictitious land-based EMSO IEMI scenario.

The figure shows different groups of habitable constructs. The area mainly comprises of residential buildings (Res) and two roads (Rd). It also incorporates infrastructure such as a "Water Works", as well as municipal buildings like a school and medical center (Med Centre), plus commercial properties in the form of industrial units (Ind), Shops, a public house (Pub), and a distribution facility (Dist). All these potentially contain victim systems of various types with various equipment properties. An "existence probability" is assigned to each victim system to model the level of certainty (i.e., reflecting the level of fuzziness in such knowledge) in whether the system exists in each specific location.

4.2. Data and SoS Elements

As can be recalled from Figure 1, the EM environment contains geographical and geological features as well as others. The model in Figure 6 includes such features in the form of buildings (for example). The relevance of these features to a QRAM model is the impact they have on the propagated transmitter power, which a QRAM must calculate because the risk to a victim system is related to the power such a system receives when the propagated power reaches the victim. If there were no materials in the path of the transmitted signal, then the calculation of received power is relatively simple, albeit it is reduced from the power at the transmitter because of attenuation caused by the physical distance between transmitter and victim (described as "Free Space Path Loss"). However, when the transmitted signal must pass through materials, then these attenuate the signal more. The QRAM enables such materials' attenuation by enabling the user to input values of attenuation rates that are assigned to the materials within each of the grid cells shown in Figure 6. Note here that while Figure 6 is only in two dimensions and uses a relatively small number of grid cells, the QRAM code does allow three-dimensional modeling

(with numbers of grid cells only limited by computing capacity) for more complex geometrical models. The signal propagation method used by the QRAM attenuates the received signal based on the attenuation properties data input by the user for all the attenuation materials the signal passes through. Such attenuation rate data are usually determined empirically and are based on the materials' composition, density, etcetera. In the model in Figure 6 (provided to demonstrate the QRAM in a readily digestible form), materials' attenuation rate data was estimated for the types of buildings described above based on various technical information sources. These data (in this case) are estimates because such buildings are formed from multiple materials and an averaging process across the grid cell is required for this. In a real-life scenario there would be uncertainty associated with the composition of such materials, which adds to the fuzzy nature of the SoS; however, a significantly more detailed geometrical model could be built where areas containing significantly fewer (maybe only one) materials are defined.

Calculating victim risk for each individual EM system, associated with victims, requires estimates of victim equipment properties. These victim equipment properties take the form of high-level parameters such as systems saturation, antenna gain, etcetera, enabling consideration of consequences beyond just component damage by enabling the modeling of failure mechanisms exceeding thresholds. While detailed knowledge of victim EM system configurations is typically unknown/unknowable, estimation of high-level equipment characteristics is possible, although information may only be known as a statistical distribution of possible values. Nevertheless, such statistically distributed equipment parameter estimates are essential because risk calculation involves estimating probabilities that victims received power levels, and frequencies cause victim equipment degradation. Because of the QRAM Monte Carlo methodology, risk assessors provide mean-value high-level victim equipment parameters and estimated statistical distributions. More details on the underlying QRAM methodology are described by Davies et al. in [63].

The location of SoS elements similarly requires statistical data to model existence probabilities for each potential piece of EM equipment belonging to a victim. These are also used in the calculation of victim risk.

4.3. Results, Validation and Verification

The methodology was tested using the fictitious land-based EW IEMI scenario described above. The risk calculations were then performed for each of the four options. The QRAM calculation results are illustrated in Figures 7–10. These demonstrate that the QRAM using an SoS model input can calculate victim risk distributions.

While the model described here is necessarily complex because it simulates a real-life scenario with unknown data, there is an underlying question over the validity of the calculated values: Do they replicate real-life values? Are they valid results?

Validation of the QRAM is not possible for several reasons, which are associated with the fuzzy, uncertain nature of the scenario knowledge, unless a dedicated facility replicating (say) an entire village was constructed with known attenuation rates for the materials for geophysical features and buildings (for example). Generally, such data, though, are only determinable using empirical measurements. Further, victim equipment properties will have uncertainties, unless equipment with known properties was used in such a facility. On the other hand, some verification is possible by using data that lead to predictable risk results in relatively simple geometrical models, although the stochastic errors associated with the Monte Carlo methodology used in the QRAM lead to some statistical variability in calculated values. This means that such verification tests also examine the impact of sampling parameters in addition to the variability of other data as already mentioned above. Nevertheless, some verification testing of the QRAM has been performed [63].

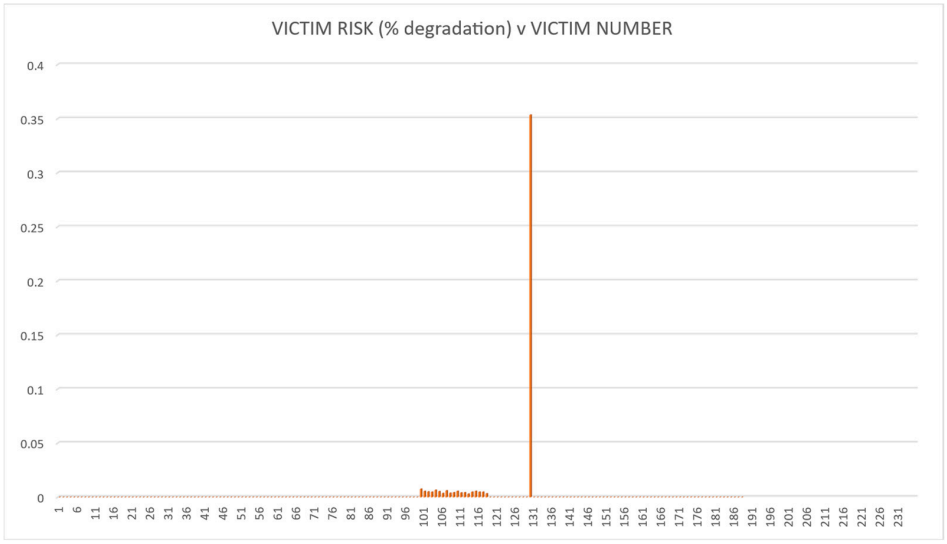

Figure 7. Victim Risk Values for Option 1.

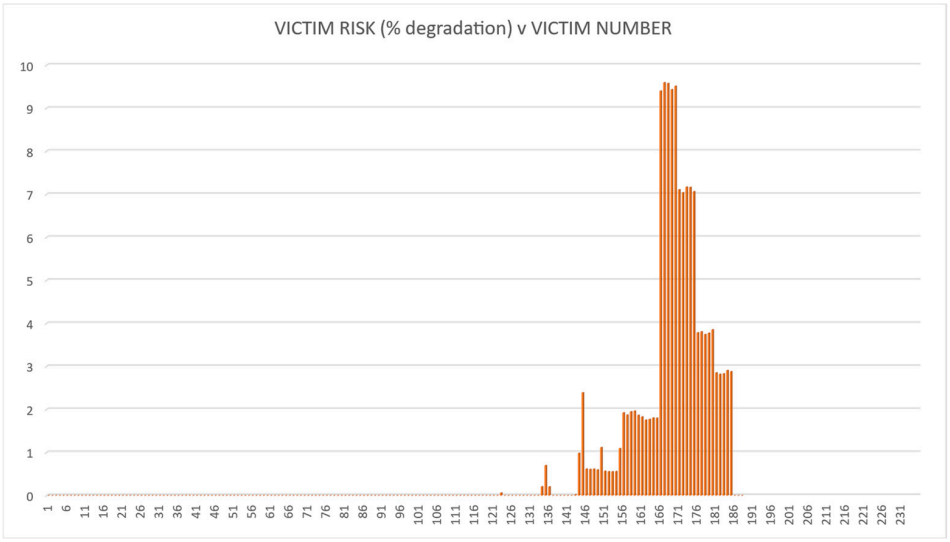

Figure 8. Victim risk values for Option 2.

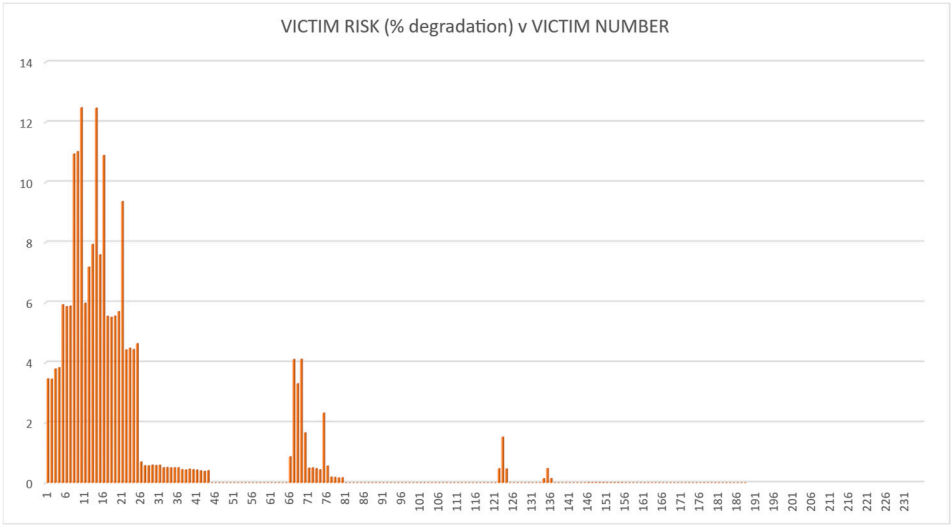

Figure 9. Victim risk values for Option 3.

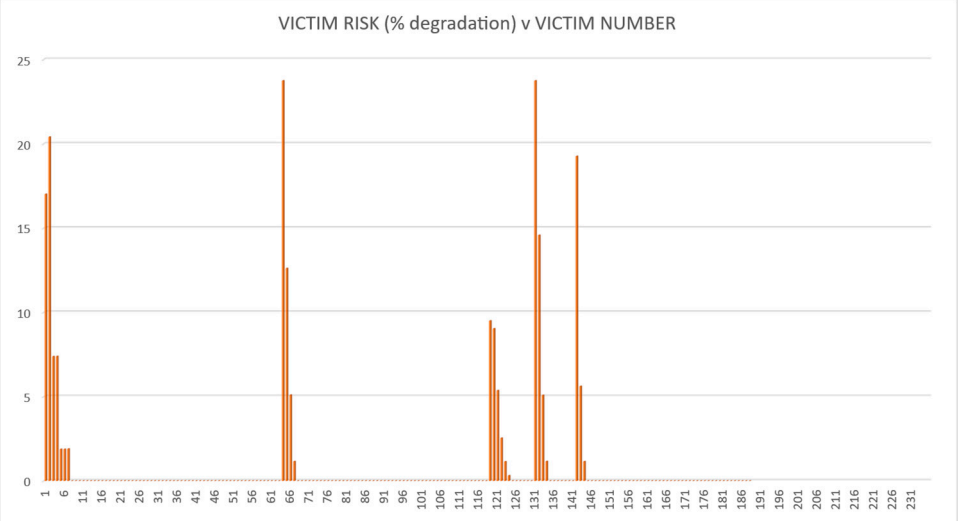

Figure 10. Victim risk values for Option 4.

5. Discussion

5.1. Relevance to SoS Types

An important aspect when discussing direct/indirect interactions (as discussed in Section 2.2 in relation to Figure 3) is particularly related to communication between system operators (i.e., those controlling EM equipment). Such communications are an important part of RA in the form of Communications and Consultations (C&C). It was also indicated above that HI is performed for purposes of gaining information. Ki-Aries et al. [65] touched on this when attempting to understand what the minimum level of information is for satisfactory security RA. In that research they worked with OASoSIS which aligns

> *"SoS factors & concepts suitable for eliciting, analyzing, validating security risks using tool-support within the SoS context"*.

They recommended

> *"alignment with a tool such as CAIRIS provides many benefits for translating operational needs into requirements"*.

In the EW IEMI RA context, increasing numbers of victims increases the complexity of the SoS. In this case, designing risk controls requires multi-stakeholder (i.e., victims) C&C. Potential failure to perform C&C efficaciously increases the probability of harm associated with

- Dynamic evolution of the SoS (changing characteristics of victims).
- Changing interoperability needs related to individual victim systems.
- Compounding emergent behaviors within the SoS (i.e., new victim interactions).

Therefore, failed C&C potentially increases risk, so C&C is an essential risk control performed by the attacker in EW IEMI RA, implying the probability (of high severity consequence in victim systems) is affected by how "good" C&C are between the transmitter and victim system owners. This further implies it is an important input to the RA harm probability calculation. The advantage of using an Acknowledged SoS model is that it enables a model for considering C&C.

Recall the discussion (in Section 2.2) on the 3 dimensions of "Resilience": "characteristics" could be interpreted as the type of SoS. Also returning to the discussions that concluded EW IEMI RA scenarios are an Acknowledged SoS, there are disadvantages with this interpretation if an alternative conclusion could be that EW IEMI RA scenarios are a mixture of SoS types. For instance, in order "to perform RA capable of calculating victim

risk distributions", the decision-maker and risk assessor construct the scenario to perform the RA and will manage their scenario model to fulfil the specific purpose of performing RA. So, despite being initially dismissed, there is some justification for arguing an EW IEMI RA scenario could be described not only as "Acknowledged" but also "Directed". Further, the discussions in Section 2.2 highlighted the important part that C&C may play in performing RA. This indicates there are aspects of a "Collaborative" SoS that also apply to EW IEMI RA scenarios. Regards "Virtual" SoS, it can be argued that at any point in time the "Designated Manager" of the EW IEMI RA scenario could change because the role of the transmitter operator may change (depending on their commander's strategy) or because enemy EM systems operators may attack the transmitter or perhaps other events modify the transmitter operator's desire to perform the operation of sending a signal to attack the target. Therefore, is it true that there is (at any time) a centralized management or purpose? While the EW IEMI RA scenario may be constructed (deliberately or accidentally) as an SoS, the SoS behavior (as viewed/anticipated from the transmitter operator for example) may change, emerging via (perhaps) informal elemental collaboration and individual element management changes.

This all suggests that the type of SoS may be transitory. So, while an EW IEMI RA scenario can be modeled as an Acknowledged SoS (as demonstrated and illustrated above) it is possible that the "Designated Management" of an Acknowledged SoS could change in an instant because of all the factors mentioned above. Thus, a given EW IEMI RA scenario may remain as (mainly) an Acknowledged SoS, but its configuration could change and "O1" could become the target, or a victim and the target could become O1, for instance. This transitory behavior suggests that defining an EW IEMI RA scenario as a specific SoS type could be described as moot.

So, returning to the discussion on "Resilience", in a static scenario, structure is relatively easy to consider because resilience for this means maintaining the type of structure shown in Figure 3 including all links and component elements. The events causing weakening of structure are illustrated in Figure 11.

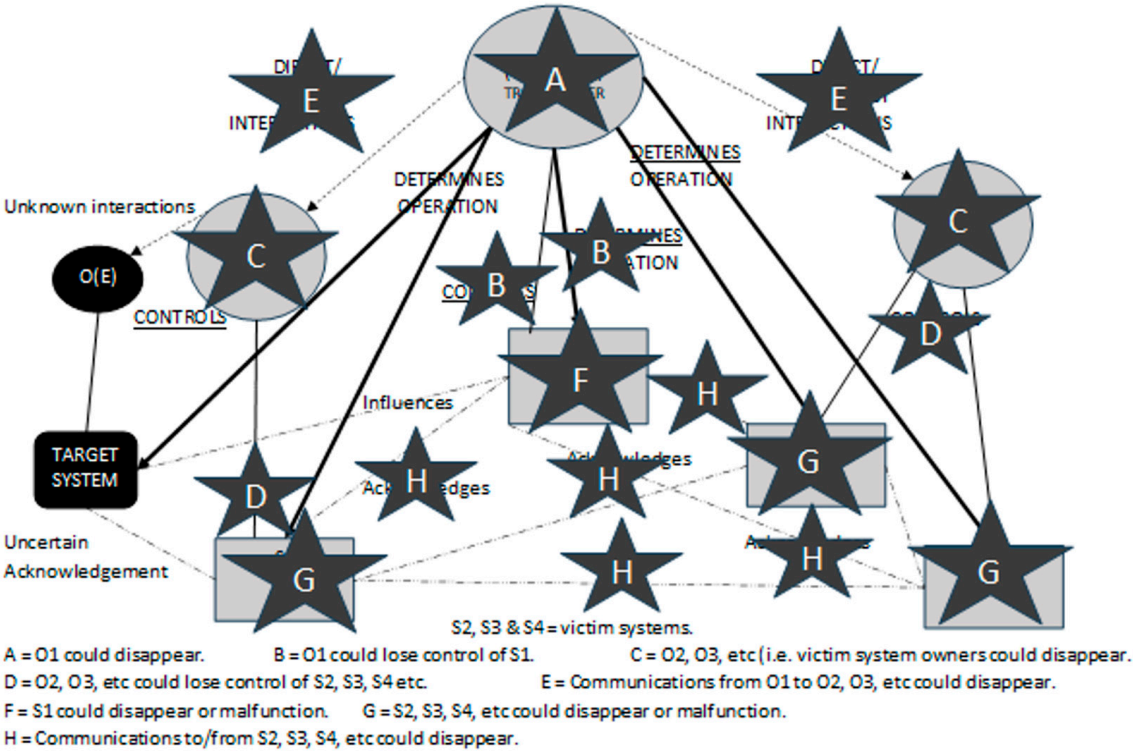

Figure 11. Events/incidents that could weaken structure.

What can be concluded is that "Resilience" does apply to whatever SoS type is assigned to an EW IEMI RA scenario, but "Resilience" is low, because "structure" can be changed without warning, and this may alter the "characteristics" of the scenario. Regards "performance" (to perform RA capable of calculating victim risk distributions), there are also potential negative impacts because of uncertainty of information. To build such uncertainty into an SoS model requires a new approach to defining SoS types. In the discussions above it was recognized that the type applying to EW IEMI RA scenarios is moot, at best an Acknowledged SoS, which nevertheless does not necessarily have well-defined elements. To encompass all this, it is recognized that what all this implies is that EW IEMI RA scenarios form a "Moot Acknowledged System-of-Fuzzy-Systems" (MASoFS). Figure 12 illustrates this by comparing a "Classic" Acknowledged SoS and one modeling an EW IEMI RA scenario.

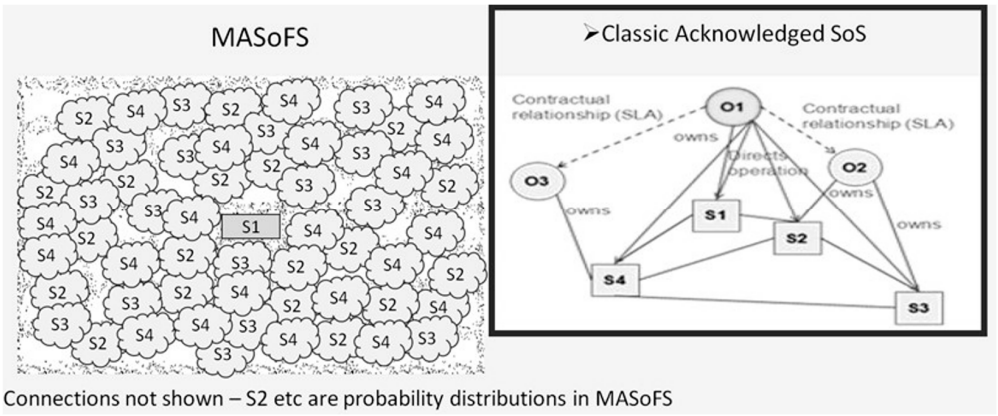

Figure 12. Moot Acknowledged System-of-Fuzzy-Systems (incorporating Dahmann [22]).

5.2. EMSO

Assuming that statistical distributions of victim equipment characteristics and existence probabilities can be estimated by a risk assessor, then the fuzzy nature of SoS elements can be modeled in the QRAM, which in turn implies that geometrically distributed victim risk values can be calculated. The Monte Carlo approach used by the QRAM also enables determination of an estimated stochastic error on victim risk values, which further enables a level of confidence to be assigned to the risk values. Sampling can be increased by the QRAM user to reduce stochastic errors.

The utilization of a MASoFS can also provide approaches to the determination of levels of C&C and hence estimation of the impacts of C&C on calculated risks. Overall, the QRAM thus provides a tool to EMSO commanders considering EW IEMI to facilitate the complex decision-making required.

6. Conclusions

This paper is a case study critically analyzing the application of SoS theory to EW IEMI RA. The particularly complex, dynamic, diverse, and uncertain environmental features of EW IEMI RA-associated scenarios led to the conclusion that there are potential configurations of these scenarios that may imply any one of the four main SoS types could apply at any point in the SoS's timeline. Because of this potential changeability (under some dynamic circumstances), a useful way of describing this is that the SoS type is moot. However, static EW IEMI RA scenarios can be modeled as an Acknowledged SoS, although the high level of uncertainty of knowledge held by attacking transmitter operators means that the constituent systems are fuzzy. This paper has therefore proposed

that a Moot Acknowledged System-of-Fuzzy-Systems (MASoFS) can be applied to EW IEMI RA scenarios.

The use of a case study with a relevant QRAM utilizing a MASoFS has demonstrated SoS theory can be applied to EW IEMI RA.

At the outset, this paper identified a knowledge gap whereby currently there is no formalized QRAM capable of calculating victim risk distributions, so a novel SoS description feeding a novel QRAM (supported by a systematic literature review of RA mathematical modeling techniques) has been proposed to address this knowledge gap, utilizing an Electromagnetic Warfare (EW) IEMI RA method modeling scenarios consisting of interacting EM systems within complex, dynamic, diverse, and uncertain environments, using Systems-of-Systems (SoS) theory.

Further work is in progress to develop a risk-informed decision-making method that utilizes quantified victim risks to enable commanders who wish to consider EW IEMI.

Author Contributions: Conceptualization, N.D., H.D. and D.K.-A.; methodology, N.D., H.D. and D.K.-A.; software, N.D.; validation, N.D.; formal analysis, N.D.; investigation, N.D.; resources, N.D., H.D. and D.K.-A.; data curation, N.D.; writing—original draft preparation, N.D.; writing—review and editing, N.D., H.D. and D.K.-A.; visualization, N.D.; supervision, H.D. and D.K.-A.; project administration, H.D.; funding acquisition, H.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Defence Science & Technology Laboratory (Dstl). Content includes material subject to © Crown copyright (2024), Dstl. This material is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3 (accessed on 3 March 2025).

Data Availability Statement: Restrictions apply to the data. The datasets presented in this article are not readily available because the data are part of an ongoing study. Requests to access the datasets should be directed to Huseyin Dogan.

Acknowledgments: To Chris Williams and Mark Osborne (both Defence Science and Technology Laboratory) for their technical support.

Conflicts of Interest: Nigel Davies reports financial support was provided by Defence Science and Technology Laboratory. Nigel Davies reports a relationship with Defence Science and Technology Laboratory that includes: funding grants. Other authors, declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Giri, D.V.; Tesche, F.M. Classification of intentional electromagnetic environments (IEMI). *IEEE Trans. Electromagn. Compat.* **2004**, *46*, 322–328.
2. Radasky, W.A.; Baum, C.A.; Wik, M.W. Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI). *IEEE Trans. Electromagn. Compat.* **2004**, *46*, 314–321. [CrossRef]
3. Sabath, F. What can be learned from documented intentional electromagnetic interference (IEMI) attacks? In Proceedings of the 2011 31th URSI General Assembly and Scientific Symposium, Istanbul, Turkiye, 13–20 August 2011.
4. Genender, E.; Mleczko, M.; Döring, O.; Garbe, H.; Potthast, S. Fault tree analysis for system modeling in case of intentional EMI. *Adv. Radio Science* **2011**, *9*, 297–302.
5. EMSOPEDIA Electro Magnetic Spectrum Operation (EMSO). Available online: https://www.emsopedia.org/entries/electromagnetic-spectrum-operation-emso/ (accessed on 2 December 2024).
6. HQ Department of the Army. *Techniques for Spectrum Management Operations, ATP 6-02.70*; HQ Department of the Army: Washington, DC, USA, 2015.
7. O'Donohue, D. *Joint Electromagnetic Spectrum Operations. Joint Publication 3-85*; U.S. Department of the Army: Washington, DC, USA, 2022.

8. Crawley, F.; Tyler, B. *Hazard Identification Methods*; Institute of Chemical Engineers: Rugby, UK, 2003.
9. Deshmukh, L.M. *Industrial Safety Management: Hazard Identification and Risk Control*; McGraw-Hill Education LLC: New York, NY, USA, 2005.
10. Mannan, S. *Lees' Process Safety Essentials: Hazard Identification, Assessment and Control*; Butterworth-Heinemann: Amsterdam, The Netherlands, 2014.
11. British Standard BS: IEC61882:2016 Hazard and Operability Studies (HAZOP Studies)—Application Guide. Available online: https://shop.bsigroup.com/ProductDetail/?pid=000000000030309555 (accessed on 29 January 2024).
12. IEC 60812:2018 Failure Modes and Effects Analysis (FMEA and FMECA). Available online: https://webstore.iec.ch/publication/26359 (accessed on 29 January 2024).
13. IEC61025:2006 Fault Tree Analysis (FTA). Available online: https://webstore.iec.ch/publication/4311 (accessed on 29 January 2024).
14. IEC 62502:2010 Analysis Techniques for Dependability—Event Tree Analysis (ETA). Available online: https://webstore.iec.ch/publication/7131 (accessed on 29 January 2024).
15. UK Civil Aviation Authority. Introduction to Bowtie. Available online: https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/About-Bowtie/Introduction-to-bowtie/ (accessed on 29 January 2024).
16. ISO/IEC/IEEE 21839:2019 Systems and Software Engineering—System of Systems (SoS) Considerations in Life Cycle Stages of a System. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:21839:ed-1:v1:en (accessed on 2 December 2024).
17. Pan, X.; Wang, H.; Yang, Y.; Zhang, G. Resilience based importance measure analysis for SoS. *J. Syst. Eng. Electron.* **2019**, *30*, 920–930.
18. Olivero, M.A.; Bertolino, A.; Dominguez-Mayo, F.J.; Escalona, M.J.; Matteucci, I. Security Assessment of Systems of Systems. In Proceedings of the IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems (SESoS) and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (WDES), Montreal, QC, Canada, 28 May 2019; pp. 62–65.
19. Silva, E.; Batista, T.; Oquendo, F. A mission-oriented approach for designing system-of-systems. In Proceedings of the 10th SoSE Conference, San Antonio, TX, USA, 17–20 May 2015; pp. 346–351. [CrossRef]
20. Chiprianov, V.; Falkner, K.; Gallon, L.; Munier, M. Towards modelling and analysing non-functional properties of systems of systems. In Proceedings of the 9th Int. Conference on SOSE, Adelaide, Australia, 9–13 June 2014; pp. 289–294.
21. Ki-Aries, D. Security Risk Assessment in Systems of Systems. Ph.D. Thesis, Bournemouth University, Bournemouth, UK, 2020.
22. Systems of Systems Characterization and Types, Dr. Judith S. Dahmann, (STO-EN-SCI-276). Available online: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-276/EN-SCI-276-01.pdf (accessed on 2 December 2024).
23. Moon, D.C.; Moon, J.; Keagy, A. Direct and Indirect Interactions. *Nat. Educ. Knowl.* **2010**, *3*, 50.
24. Xiao, Y.; Watson, M. Guidance on Conducting a Systematic Literature Review. *J. Plan. Educ. Res.* **2019**, *39*, 93–112.
25. PRISMA. Welcome to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Website. Available online: http://prisma-statement.org/ (accessed on 2 December 2024).
26. Fourie, W. Leadership and risk: A review of the literature. *Leadersh. Organ. Dev. J.* **2022**, *43*, 550–562. [CrossRef]
27. Shukla, A.; Katt, B.; Nweke, L.O.; Yeng, P.K.; Weldehawaryat, G.K. System security assurance: A systematic literature review. *Comput. Sci. Rev.* **2022**, *45*, 100496. [CrossRef]
28. Syafitri, W.; Shukur, Z.; Mokhtar, A.U.; Sulaiman, R.; Ibrahim, M.A. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 39325–39343. [CrossRef]
29. Alouffi, B.; Hasnain, M.; Alharbi, A.; Alsosaimi, W.; Alyami, H.; Ayaz, M. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access* **2021**, *9*, 57792–57807. [CrossRef]
30. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156.
31. Lisova, E.; Šljivo, I.; Čaušević, A. Safety and Security Co-Analyses: A Systematic Literature Review. *IEEE Syst. J.* **2019**, *13*, 2189–2200.
32. Nelson, B.; Olovsson, T. Security and Privacy for Big Data: A Systematic Literature Review. In Proceedings of the 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 5–8 December 2016; pp. 3693–3702.
33. Harvard Countway Library. Systematic Reviews and Meta Analysis. Available online: https://guides.library.harvard.edu/meta-analysis/GettingStarted (accessed on 29 January 2024).
34. Bournemouth University. Systematic Reviews—Searching for Literature: Introduction. Available online: https://libguides.bournemouth.ac.uk/c.php?g=471700&p=3225871 (accessed on 29 January 2024).
35. Mao, C.; Canavero, F. System-Level Vulnerability Assessment for EME: From Fault Tree Analysis to Bayesian Networks-Part I: Methodology Framework. *IEEE Trans. Electromagn. Compat.* **2016**, *58*, 180–187.
36. Genender, E.; Garbe, H.; Sabath, F. Probabilistic risk analysis technique of intentional electromagnetic interference at system level. *IEEE Trans. Electromagn. Compat.* **2014**, *56*, 200–207.
37. Liu, Y.; Du, P.; Han, F.; Xia, H.; Wang, J. A Bayesian Estimation of Confidence Limits for Multi-state System Vulnerability Assessment With IEMI. *IEEE Trans. Electromagn. Compat.* **2022**, *64*, 1219–1229.

38. Liu, Y.; Han, F.; Wang, J.; Qi, H. Vulnerability assessment of a multistate component for IEMI based on a Bayesian method. *IEEE Trans. Electromagn. Compat.* **2019**, *61*, 467–475. [CrossRef]
39. Houret, T.; Besnier, P.; Vauchamp, S.; Pouliguen, P. Probability of Failure Using the Kriging-Controlled Stratification Method and Statistical Inference. In Proceedings of the 2020 International Symposium on Electromagnetic Compatibility—EMC EUROPE, EMC EUROPE 2020, Online, 23–25 September 2020; p. 9245860.
40. Sabath, F. EMI risk management with the threat scenario, effect, and criticality analysis. In *Ultra-Wideband Short-Pulse Electromagnetics*; Springer: New York, NY, USA, 2014; Volume 10, pp. 265–278.
41. Mondal, S.K.; Tan, T.; Khanam, S.; Kabir, H.M.D.; Ni, K. Security Quantification of Container-Technology-Driven E-Government Systems. *Electronics* **2023**, *12*, 1238. [CrossRef]
42. Peikert, T.; Garbe, H.; Potthast, S. A fuzzy approach for IEMI risk analysis of IT-Systems with respect to transient disturbances. In Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, Dresden, Germany, 16–22 August 2015; pp. 1077–1082.
43. Peikert, T.; Garbe, H.; Potthast, S. Risk analysis with a fuzzy-logic approach of a complex installation. *Adv. Radio Sci.* **2016**, *14*, 91–96.
44. Peikert, T.; Garbe, H.; Potthast, S. Fuzzy-Based Risk Analysis for IT-Systems and Their Infrastructure. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1294–1301.
45. Liwang, H.; Ericson, M.; Bang, M. An examination of the implementation of risk-based approaches in military operations. *J. Mil. Stud.* **2014**, *5*, 38–64.
46. Paltrinieria, N.; Comfort, L.; Reneirs, G. Learning about risk: Machine learning for risk assessment. *Saf. Sci.* **2019**, *118*, 475–486. [CrossRef]
47. Pasman, J.; Rogers, W.J.; Mannan, M.S. Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Saf. Sci.* **2017**, *99*, 140–155.
48. Rawson, A.; Brito, M.; Sabeur, Z.; Tran-Thanh, L. From Conventional to Machine Learning Methods for Maritime Risk Assessment. *Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 757–764. [CrossRef]
49. Choi, S.; Kwon, O.-J.; Oh, H.; Shin, D. Method for effectiveness assessment of electronic warfare systems in cyberspace. *Symmetry* **2020**, *12*, 2107. [CrossRef]
50. Devaraj, L.; Ruddle, A.R.; Duffy, A.P. EMI Risk Estimation for System-Level Functions Using Probabilistic Graphical Models. In Proceedings of the Joint IEEE International Symposium on Electromagnetic Compatibility Signal and Power Integrity, and EMC Europe, EMC/SI/PI/EMC Europe 2021, Virtual, 26 July–20 August 2021; pp. 851–856.
51. Mansson, D.; Thottappillil, R.; Backstrom, M. Methodology for classifying facilities with respect to intentional EMI. *IEEE Trans. Electromagn. Compat.* **2009**, *51*, 46–52. [CrossRef]
52. Ruddle, A.R. Risk Analysis for Automotive EMC: Scope, Approaches and Challenges. In Proceedings of the 2020 International Symposium on Electromagnetic Compatibility—EMC EUROPE 2020, Online, 23–25 September 2020; p. 9245774.
53. Devaraj, L.; Ruddle, A.R.; Duffy, A.P. System Level Risk Analysis for Immunity in Automotive Functional Safety Analyses. In Proceedings of the 2020 International Symposium on Electromagnetic Compatibility—EMC EUROPE 2020, Online, 23–25 September 2020; p. 9245692.
54. Li, K.-J.; Xie, Y.-Z.; Chen, Y.-H.; Zhou, Y.; Hui, Y.-C. Bayesian inference for susceptibility of electronics to transient electromagnetic disturbances with failure mechanism Consideration. *IEEE Trans. Electromagn. Compat.* **2020**, *62*, 1669–1677.
55. Zhou, P.; Lv, Y.; Chen, Z.; Xu, H. System-level EMC assessment for military vehicular communication systems based on a modified four-level assessment model. *China Commun.* **2018**, *15*, 39–53.
56. Xu, T.; Chen, Y.; Wang, Y.; Zhang, D.; Zhao, M. EMI Threat Assessment of UAV Data Link Based on Multi-Task CNN. *Electronics* **2023**, *12*, 1631. [CrossRef]
57. Jang, J.; Kim, K.; Yoon, S.; Lee, S.; Ahn, M.; Shin, D. Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated with Cyber Asset Damage. *IEEE Access* **2023**, *11*, 45113–45128.
58. Butt, F.A.; Jalil, M. An overview of electronic warfare in radar systems. In Proceedings of the International Conference on Technological Advances in Electrical, Electronics and Computer Engineering, Konya, Turkey, 9–11 May 2013; pp. 213–217.
59. Howard, C.; Stumptner, M. Probabilistic reasoning techniques for situation assessments. In Proceedings of the 3rd International Conference on Information Technology and Applications, Sydney, NSW, Australia, 4–7 July 2005; pp. 383–386.
60. Salnikova, O.; Cherviakova, O.; Sova, O.; Zhyvotovskyi, R.; Petruk, S.; Hurskyi, T.; Shyshatskyi, A.; Nos, A.; Neroznak, Y.; Proshchyn, I. Development of an improved method for finding a solution for neuro-fuzzy expert systems. *East.-Eur. J. Enterp. Technol.* **2020**, *5*, 35–44.
61. Sova, O.; Shyshatskyi, A.; Malitskyi, D.; Zhuk, O.; Gaman, O.; Hordiichuk, V.; Fedoriienko, V.; Kokoiko, A.; Shevchuk, V.; Sova, M. Development of a complex method for finding a solution for neuro-fuzzy expert systems. *East.-Eur. J. Enterp. Technol.* **2020**, *6*, 22–31.
62. Taherdoost, H.; Madanchian, M. Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia* **2023**, *3*, 77–87. [CrossRef]

63. Davies, N.; Williams, C.; Osborne, M.; Dogan, H.; Ki-Aries, D.; Jiang, N. Electromagnetic Warfare Intentional Interference: Victim Risk Assessment. *IEEE Trans. EMC* 2025, *submitted*.
64. de Vries, J.P. An Outline of Risk-Informed Interference Assessment. Available online: https://ssrn.com/abstract=2564213 (accessed on 2 December 2024).
65. Ki-Aries, D.; Faily, S.; Dogan, H.; Williams, C. Assessing System of Systems Security Risk and Requirements with OASoSIS. In Proceedings of the IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE), Banff, AB, Canada, 20 August 2018; pp. 14–20.