Alexandria Engineering Journal 78 (2023) 561–575

Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original Article

A TEMPEST vulnerability prediction method for cyber security practitioners

Maxwell Martin [*], Funlade Sunmola, David Lauder

School of Physics, Engineering and Computer Science, University of Hertfordshire, Hatfield AL10 9AB, UK

ARTICLE INFO

Keywords:
Unintentional Emanations
TEMPEST
Fuzzy logic
Vulnerability assessment

ABSTRACT

Sensitive information can have its security compromised by unintentional electromagnetic emissions from the information technology equipment (ITE) being used to process it. It is important to assess the likelihood of a potential compromise, and this requires radio frequency (RF) engineering expertise to predict the likelihood of the vulnerability occurring. This paper describes the development of a fuzzy inference system that can be used to assess the radiated and conducted vulnerability likelihood of unintentional electromagnetic emanations. The system has the potential to be a valuable tool for cybersecurity practitioners without RF expertise. The system has been tested on office-based ITE devices, and it is effective in predicting the likelihood of radiated and conducted vulnerabilities occurring. Areas of future work include extending the fuzzy inference system to use RF propagation models and enabling it to make vulnerability likelihood predictions after countermeasures have been applied.

1. Introduction

Electromagnetic compatibility (EMC) standards [1] ensure that electronic products do not create unacceptable levels of electromagnetic interference and are immune to interference from other electronic devices. This helps to protect the security objectives of integrity and availability. However, it does not necessarily protect the security objective of confidentiality. The electromagnetic fields generated by information technology equipment (ITE) when it is operated can give rise to unintentional emanations. These emanations can radiate into space or conduct along power and signal lines. If these emanations are related to the information being processed, they can be captured and reconstituted, leading to a loss of confidentiality. This vulnerability is known as TEMPEST [2].

In 1985, [3] demonstrated, for the first time publicly, how to eavesdrop on a computer monitor's display. This showed that office-based electronic equipment can emit electromagnetic radiation that can be used to steal sensitive information. By identifying the two main types of radiated signals as clocks and video emissions it also demonstrated that EMC standards are not enough to protect against TEMPEST attacks. Research studies that have followed continue to show that TEMPEST vulnerabilities persist. For example, computer monitors [4], wired and wireless keyboards [5], and touch screens [6] have all been shown to be vulnerable to TEMPEST attacks. Research has also shown that radiated emissions from TEMPEST attacks can be recovered up to 300 m away and that conducted emissions can travel still greater distances [7]. This indicates that TEMPEST vulnerabilities are still a serious threat to the confidentiality of sensitive information.

Research has also enhanced our understanding of the mechanisms that produce TEMPEST vulnerabilities and how to mitigate them. This research has shown that electronic components and circuit boards can act as antennas and that by careful redesign of component layout, and the use of decoupling, filtering and shielding it is possible to reduce their effects [8]. An outcome of this research is the recognition that TEMPEST vulnerabilities need to be considered throughout the entire lifecycle of a system, from design and manufacture to testing and quality assurance. This is because even minor differences in manufacturing quality can lead to unintentional emanations that could be exploited by attackers. One way to mitigate TEMPEST vulnerabilities is to certify equipment against international standards [9]. This ensures that the equipment has been manufactured to a high quality and meets certain security requirements. However, this can increase the cost of the equipment, which can drive project procurement decisions towards commercial off-the-shelf (COTS) equipment. As a result, it is important to carefully consider the security implications of using COTS equipment in sensitive environments.

The focus of research into TEMPEST has traditionally been on office-

[*] Corresponding author.
E-mail address: m.e.martin@herts.ac.uk (M. Martin).

https://doi.org/10.1016/j.aej.2023.07.059
Received 10 February 2023; Received in revised form 4 June 2023; Accepted 24 July 2023
Available online 3 August 2023

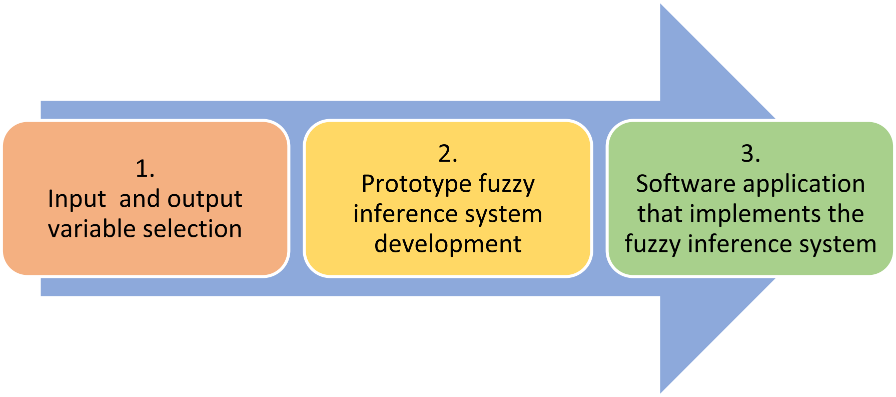

1.
Input and output variable selection
2.
Prototype fuzzy inference system development
3.
Software application that implements the fuzzy inference system

Fig. 1. Methodology.

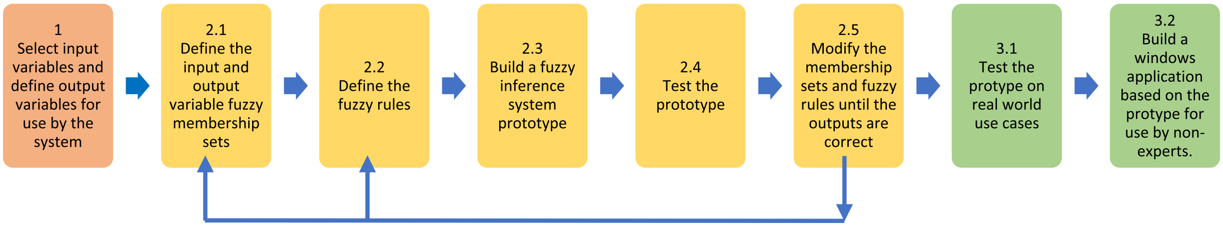

1
Select input variables and define output variables for use by the system
2.1
Define the input and output variable fuzzy membership sets
2.2
Define the fuzzy rules
2.3
Build a fuzzy inference system prototype
2.4
Test the prototype
2.5
Modify the membership sets and fuzzy rules until the outputs are correct
3.1
Test the protype on real world use cases
3.2
Build a windows application based on the protype for use by non-experts.

Fig. 2. FIS development stages.

Table 1
Vulnerability Factors.

ID	Factor	Description
V1	ITE Geolocation	Level of challenge in ITE operating environment.
V2	Physical Security	Physical security access controls.
V3	Inspectable Space	Distance between attacker and ITE.
V4	Countermeasures	Radiated and conducted emanation countermeasures.
V5	Ambient Interference and Radio Noise	Ambient interference and radio noise.
V6	ITE Radiation Profile	Distance ITE radiates.
V7	ITE Interfaces	ITE interfaces.
V8	ITE Interface Cable Connections	Using the correct interface cable connections.
V9	Cable Distribution Facilities	Cable layout and separation distances.
V10	Application of Installation Standards	Applying installation standards
V11	Facility Power Consumption	Power consumed by the facility.
V12	Building Construction	RF Attenuation from building materials.
V13	Transmitters	Transmitter effects on ITE operating environment.
V14	Policy / Standards / Guidelines	Adhering to policy/standards/guidelines.
V15	ITE Type	Selecting appropriate ITE.
V16	Configuration and Control	Managing and controlling change.
V17	Size of ITE Installation	Number of ITE deployed.
V18	ITE Supply Chain	Using a trusted ITE supply chain.
V19	Radio Frequency Monitoring	Monitoring the RF environment.

Table 2
Vulnerability factors used as inputs to the FIS.

ID	Input	Related Vulnerability Factor	Description
I1	ITE Physical and Supply Chain Security	V2 Facility Physical Security V18 ITE Supply Chain	Assessment of how secure the ITE is, both physically and from a supply chain perspective.
I2	ITE Radiation Distance	V8 ITE Cable Connections V15 ITE Type	Assessment of the distance the ITE will radiate based on its type and connections (i.e., whether they are shielded, mixed or unshielded).
I3	Distance from ITE to the secure perimeter	V3 Inspectable Space (IS)	Assessment of the nearest distance from which emanations could be captured.
I4	Size of Installation	V17 Size of Installation	Assessment of the number of ITEs used in the installation.
I5	Utility Lines leaving the Secure Perimeter	V9 Cable Distribution Facilities	Assessment of whether any utility lines (power or signal) connected to the ITE installation leave the secure perimeter.

based ITE. However, the Internet of Things (IoT) is a rapidly growing technology sector with ~15 billion networked IoT devices by the year 2023 [10]. This brings new challenges, primarily around scale, as many of these devices will use the same Internet protocols to connect, and will therefore be open to new and established system and network attacks. Authentication of IoT endpoint devices (sensors and actuators) into the wider network, may introduce opportunities for TEMPEST attacks. Wireless sensor networks, vehicle communications, medical devices [11], and cyber-physical human systems employ authentication mechanisms with different levels of sophistication depending on the resources at their disposal. For example, a sensor to measure a physical quantity may have limited resources in terms of electronics and power [12]. This has implications in terms of attack vectors. For example, it may be easier to attack certain IoT devices because they are easier to gain physical access to. As a result, it is also important to carefully consider the security implications of using IoT devices along with office-based ITE in sensitive environments.

The increased use of technology and continuing technical innovations though beneficial also have the drawback of creating more vulnerabilities and also providing would-be attackers with greater access to technologies previously not available to them. It is now possible with a modest budget to procure software-defined radios, signal processing software and RF test equipment to launch TEMPEST attacks. This means, TEMPEST vulnerabilities, like other cyber vulnerabilities, need to be risk-managed [13]. This requires knowledge of the threats and their capabilities, as well as the vulnerabilities of the organization's

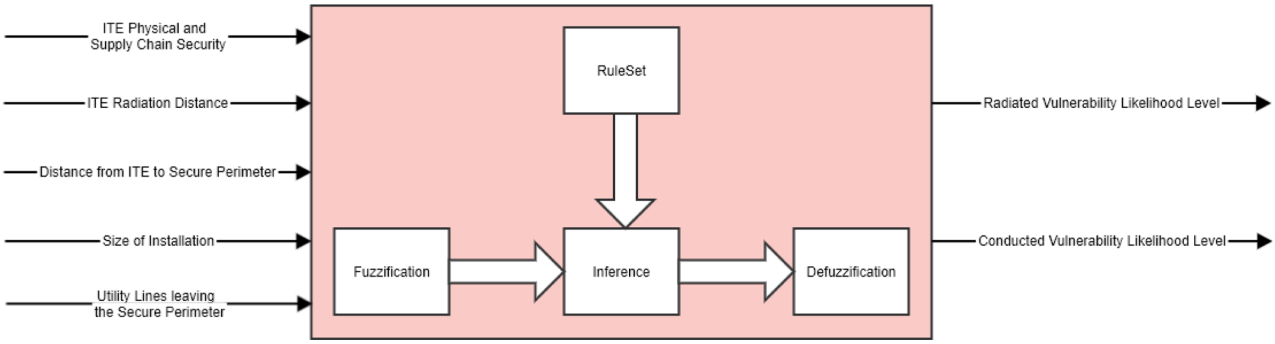
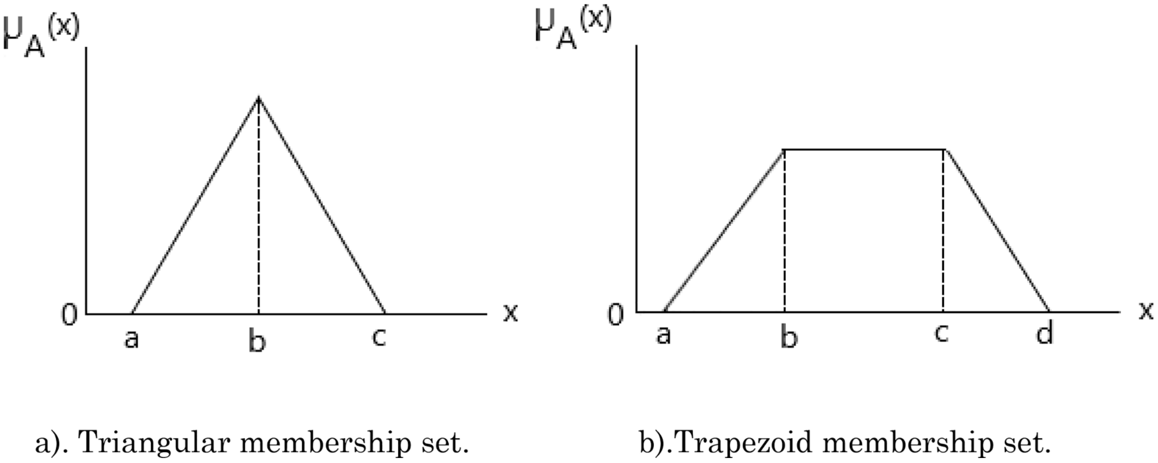

ITE Physical and Supply Chain Security
ITE Radiation Distance
Distance from ITE to Secure Perimeter
Size of Installation
Utility Lines leaving the Secure Perimeter
RuleSet
Fuzzification
Inference
Defuzzification
Radiated Vulnerability Likelihood Level
Conducted Vulnerability Likelihood Level

Fig. 3. Stages of a fuzzy inference process.



a). Triangular membership set.

b).Trapezoid membership set.

Fig. 4. Membership functions.

Table 3
FIS input and output fuzzy membership sets.

ID	Input	Fuzzy Membership Set	Range
I1	ITE Physical and Supply Chain Security	Secure / Partially Secure / Insecure	0–5
I2	ITE Radiation Distance	Short / Medium / Far	0–150
I3	Distance from ITE to the secure perimeter	Short / Medium / Far	0–150
I4	Size of Installation	Small / Medium / Large	1–150
I5	Utility Lines leaving the Secure Perimeter	None / Some / All	0–5
	Output	**Fuzzy Membership Set**	**Range**
O1	Radiated Vulnerability Likelihood Level	Very Unlikely / Unlikely / Possible / Likely / Very Likely	0–1
O2	Conducted Vulnerability Likelihood Level	Very Unlikely / Unlikely / Possible / Likely / Very Likely	0–1

people, processes, and technology. It also requires an understanding of the detrimental impacts on an organisation's business should the organization's information or systems be compromised. It can be difficult for cybersecurity practitioners without appropriate and relevant radio frequency (RF) engineering experience to assess the severity of these vulnerabilities within the wider cyber vulnerability context. In practice, this means there is a reliance on RF expertise to quantify the likelihood of exploitation [14].

The assertion that the dependency on RF engineers must be removed or at least minimised because RF engineers with TEMPEST expertise are in short supply is difficult to prove. For example in the United Kingdom, the classification of engineering professions does not identify RF engineering specifically, and as a profession, it is likely to fall under the groupings of electronic and telecommunication engineering. However, there are some indicators, such as current RF engineering vacancies [15], the small number of companies that are certified to carry out TEMPEST-related work [16] and the general state of supply and demand in the engineering profession [17], that support this assertion. Therefore, to minimise this dependency it would be useful if security practitioners without RF expertise could assess the level of radiated and conducted vulnerability before engaging with external RF consultancy services. This would potentially save time and money, especially where

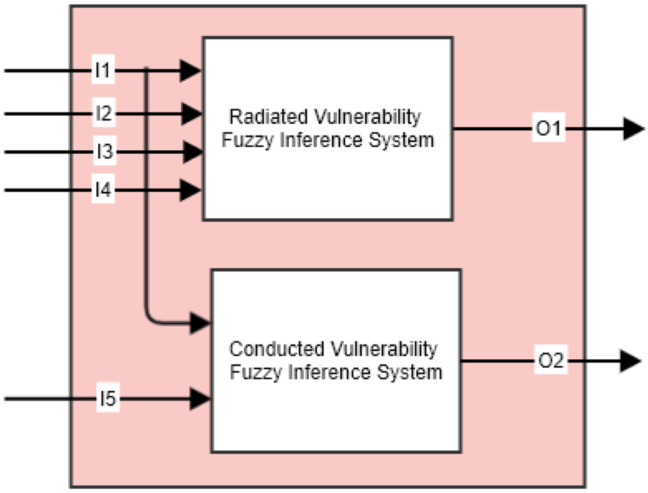
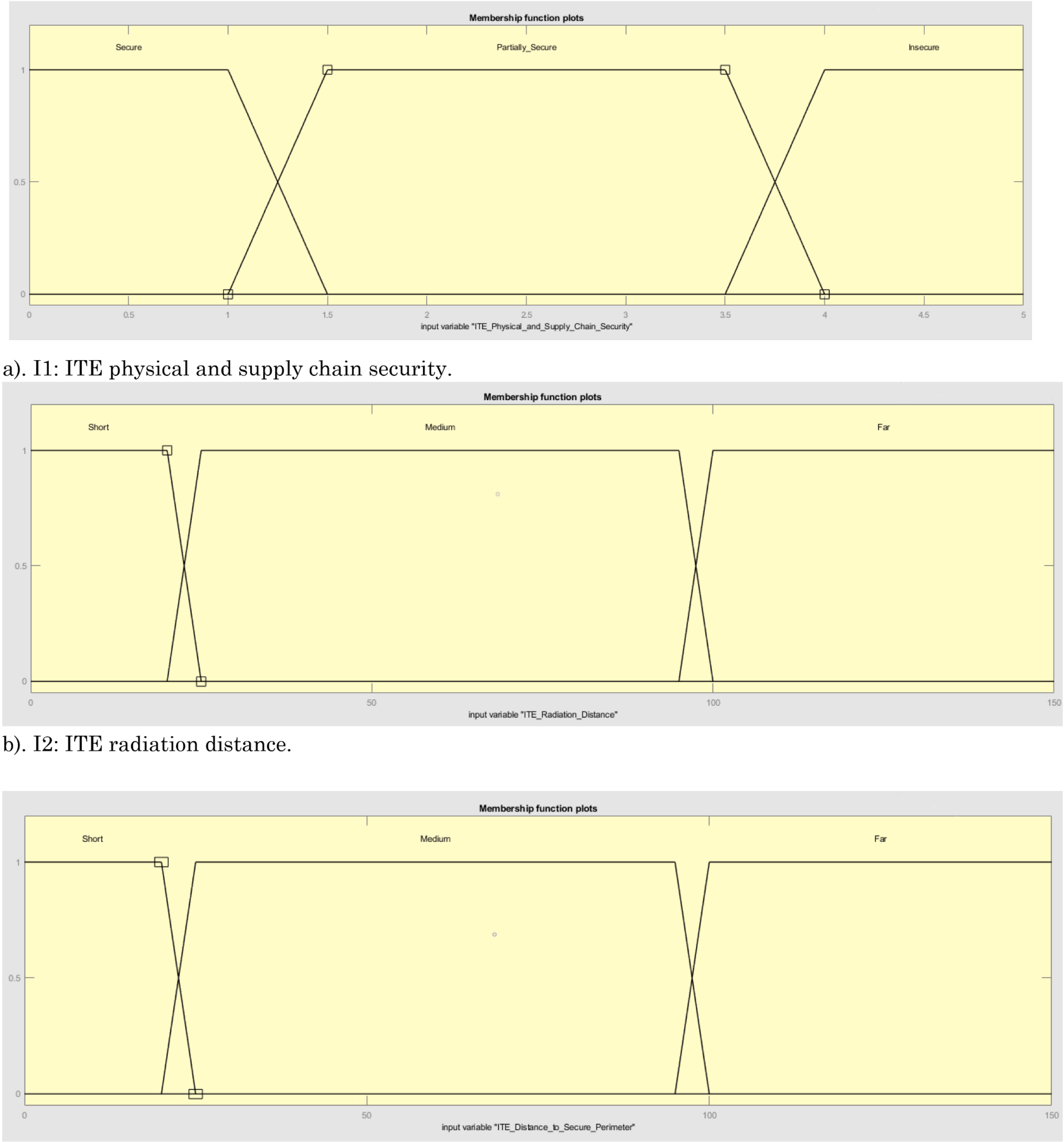

I1
I2
I3
I4
I5
Radiated Vulnerability Fuzzy Inference System
Conducted Vulnerability Fuzzy Inference System
O1
O2

Fig. 5. Implementation of the Fuzzy Inference System.



a). I1: ITE physical and supply chain security.

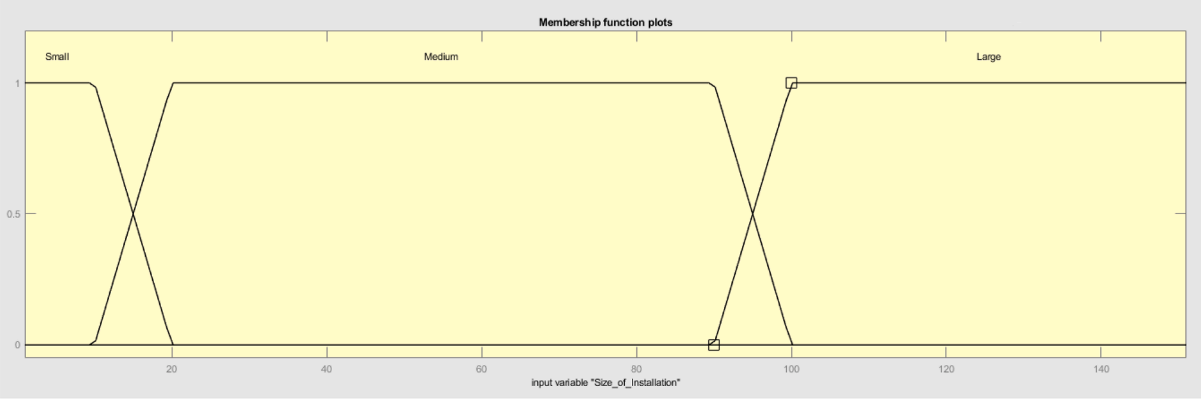
b). I2: ITE radiation distance.

c). I3: ITE distance to secure perimeter.

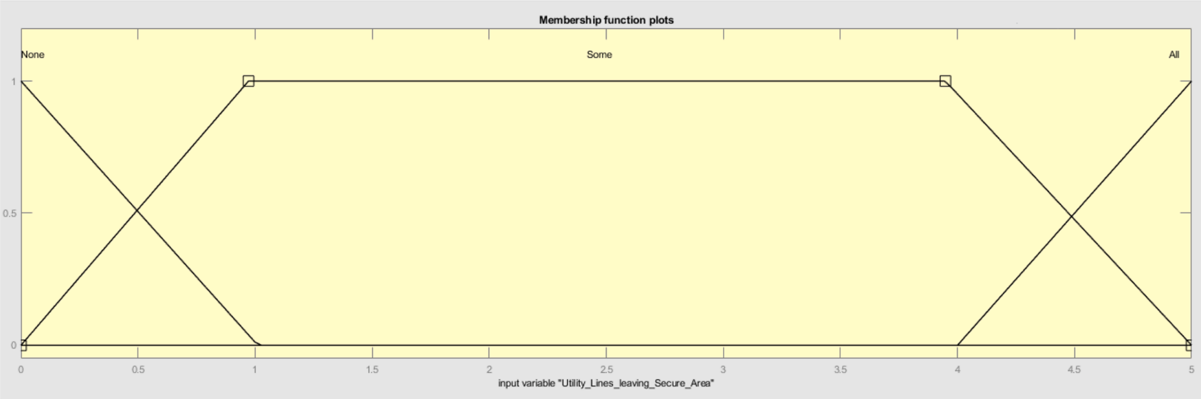
Fig. 6. FIS membership sets.

an organisation was establishing an information security management system such as ISO27001 [18] and wanted to determine appropriate mitigation to manage its risk from electromagnetic leakage of information.

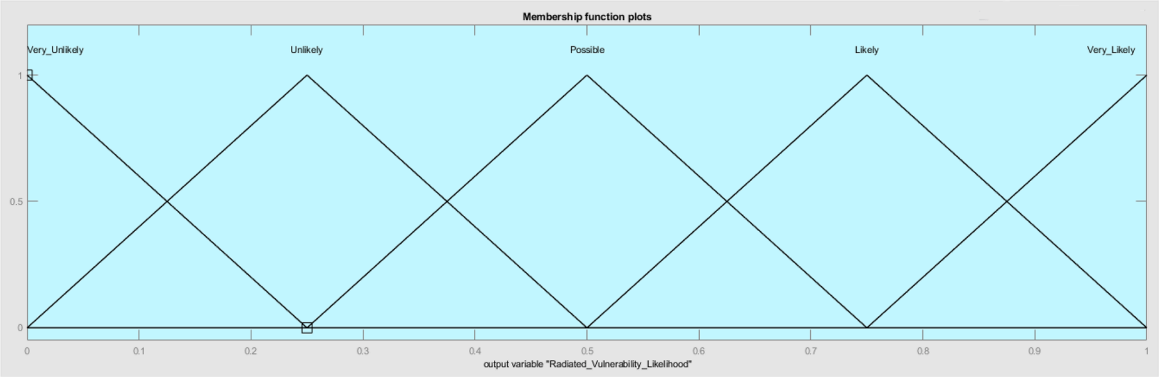
Although there has been considerable research on software vulnerability prediction models in the context of ITE and information and cyber security [19]. There is a lack of research on using prediction models for determining the likelihood of ITE exhibiting electromagnetic radiated and conducted vulnerabilities. Whether the prediction model is used for software development or electromagnetic vulnerabilities, confidence in the model's ability to make reliable predictions is a fundamental precondition of its acceptance and use [20]. A range of statistical and soft computing techniques have been used to predict software reliability [21]. Some of these techniques, particularly the computational ones using neural networks and fuzzy logic are more amenable to conditions of uncertainty. Hybrid approaches such as neural-fuzzy networks have also been tried when attempting to predict software reliability [22]. In the case of electromagnetic radiation, there is considerable uncertainty in predicting the distance an emission will travel without access to ITE test results. This means an RF expert asked to predict the vulnerability likelihood will need to draw on their experience and expertise to consider the equipment in the context of its deployment. Given the dependence on RF experts and the use of their knowledge when assessing the vulnerability likelihood, any approach



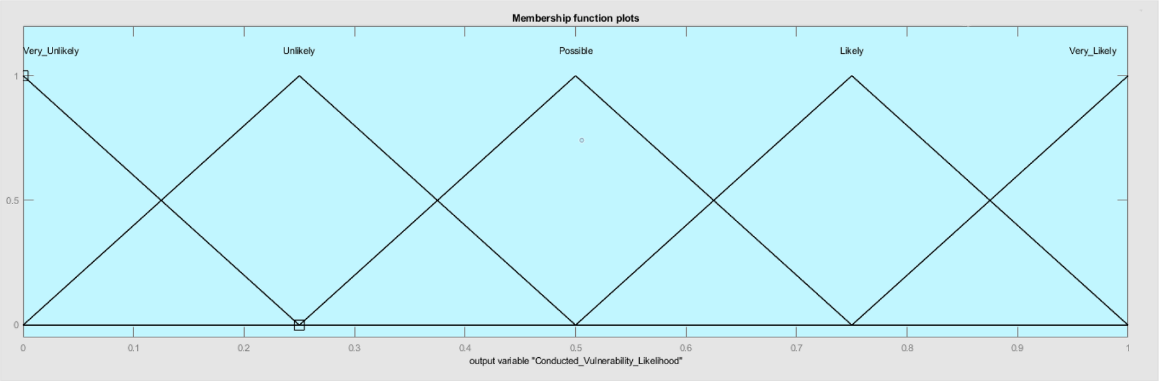
d). I4: Size of installation.



e). I5: Utility lines leaving secure perimeter.

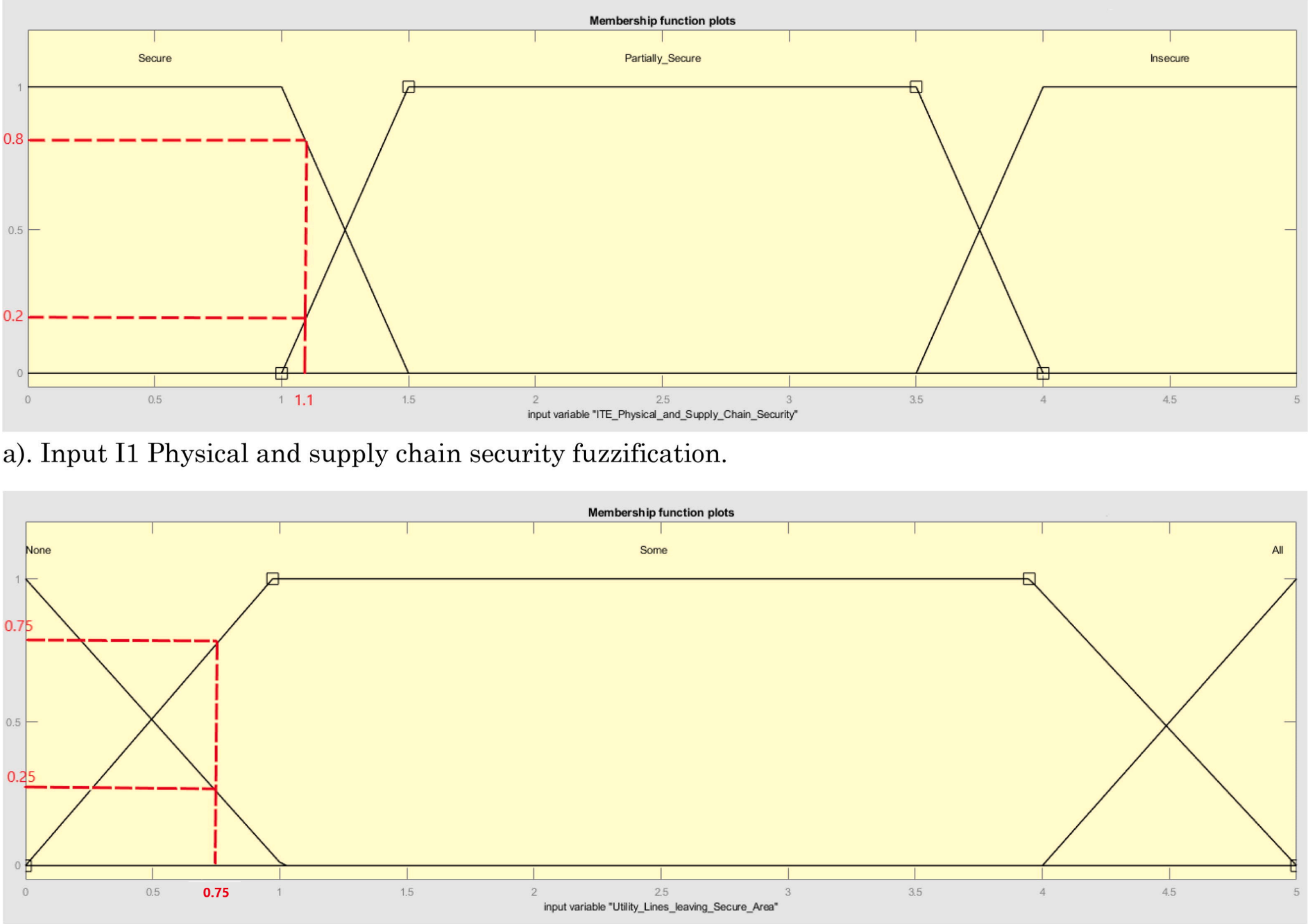


f). O1: Radiated vulnerability likelihood.



g). O2: Conducted vulnerability likelihood.

Fig. 6. (*continued*).



a). Input I1 Physical and supply chain security fuzzification.

b). Input I5 Utility lines leaving the secure perimeter fuzzification.

Fig. 7. Fuzzification of input values.

selected to enable a prediction would need to be able to cope with the vagueness and imprecision present when eliciting and expressing expert knowledge [23]. Thus, allowing expert reasoning to be expressed in terms that are understandable to non-experts. Therefore, this paper proposes a TEMPEST radiated and conducted vulnerability likelihood prediction using a fuzzy logic approach.

Fuzzy logic or fuzzy set theory as originally described by Latfi Zadeh in 1965 [24], accommodates the cases where sharp criteria cannot be used to classify the membership of an object within a specific set. In the real-world objects have graduations of membership of specific sets, fuzzy logic enables this graduation to be handled, such as when trying to assess the likelihood of events occurring. Since its introduction fuzzy logic has been used extensively in engineering-led applications, particularly related to control of industrial processes, medical instrumentation such as blood pressure monitors and consumer products from flow control in showers to car braking systems. More recently there has been a broadening of the fuzzy systems developed to include non-engineering applications where decisions and predictions need to be reached [25]. Some of these systems are safety critical and need to make decisions in real-time [262728]. The temporal aspects bring additional challenges, such as how to structure systems that incorporate fuzzy logic rule bases to enable them to deal with input variable changes in real-time e.g. from sensors, such that the system can respond appropriately when needed. Additionally, some scenarios for real-time systems will require the fuzzy logic rule base to be modified. This means learning algorithms [29] will also need to be incorporated, increasing the complexity of any system developed.

The prediction approach developed using fuzzy logic in this study, determined the radiated and conducted vulnerability likelihood from unintentional emanations before any mitigation was applied. It achieved this by using vulnerability factors as inputs. Earlier research had identified and modelled the causal factors that RF engineers consider when assessing these types of vulnerabilities from office-based ITE, i.e., thin client workstations [30]. A subset of these factors was used as the input in this study.

The remaining sections of this paper are structured as follows. Section 2 details the research methodology, using RF experts to identify the relevant vulnerability factors and to define the fuzzy membership sets and rule bases that underpin the prediction approach. Section 3 contains the results, showing how the model performed against the real-world test cases provided by the RF experts. Section 4 discusses the results obtained. The paper concludes and suggests areas of future work in Section 5.

2. Methodology

This study uses a fuzzy logic approach to predict the TEMPEST vulnerability likelihood. The model is implemented using a fuzzy inference system (FIS) that can predict the likelihood of radiated and conducted vulnerabilities occurring in office-based information technology equipment (ITE).

When considering vulnerability likelihood, we can define a set of classes (e.g., very unlikely, unlikely, possible, likely, and very likely) and measure or assess outcomes so that we can attribute them to a particular set. If we let *PL* be the universe of all possible likelihoods and denote the elements belonging to this universe as *pl*. Then in classical set theory, a

Table 4
Radiated vulnerability FIS outcome conditions.

Input condition				Output condition	
I1	I2	I3	I4	O1	Rule
Secure	Short	Short	Small	Likely	10
			Medium	Possible	5
			Large	Possible	
		Medium	Small	Possible	6
			Medium	Unlikely	2
			Large	Unlikely	
		Far	Small	Unlikely	3
			Medium	Very Unlikely	1
			Large	Very Unlikely	
	Medium	Short	Small	Very Likely	17
			Medium	Likely	11
			Large	Likely	
		Medium	Small	Likely	12
			Medium	Possible	7
			Large	Possible	
		Far	Small	Possible	8
			Medium	Unlikely	4
			Large	Unlikely	
	Far	Short	Small	Very Likely	18
			Medium	Likely	13
			Large	Likely	
		Medium	Small	Very Likely	19
			Medium	Likely	14
			Large	Likely	
		Far	Small	Likely	15
			Medium	Possible	9
			Large	Possible	
Partially Secure	Don't care (X)	X	X	Likely	16
Insecure	X	X	X	Very Likely	20

Table 5
Conducted vulnerability FIS outcome conditions.

Input condition		Output condition	
I1	I5	O2	Rule
Secure	None	Very Unlikely	1
	Some	Possible	3
	All	Possible	
Partially Secure	None	Unlikely	2
	Some	Likely	5
	All	Likely	
Insecure	None	Possible	4
	Some	Very Likely	6
	All	Very Likely	

crisp set $VL = \{very\ likely\ outcome\}$ within PL, is defined by a function $f_{VL}(pl)$. We can then define the membership of $f_{VL}(pl)$, such that if the likelihood of an event is considered very likely it belongs in the set $f_{VL}(pl) = 1$, otherwise it doesn't belong and $f_{VL}(pl) = 0$. The problem with this is that we need to define some crisp threshold for an outcome to be designated very likely, as shown by equation (1).

$$f_{VL}(pl) = \begin{cases} 1, & if\ \ pl \in VL \\ 0, & if\ \ pl \notin VL \end{cases} \cdots\cdots\cdots \tag{1}$$

However, in fuzzy logic, a fuzzy set $VL = \{very\ likely\ outcome\}$ within PL, is defined by a membership function $\mu_{VL}(pl)$, which allows for graduations of membership between 0 and 1, as shown by equation (2). Unlike the classical crisp set where something belongs, or it does not.

$$\mu_{VL}(pl) = \begin{cases} 1, if\ \ pl\ \ is\ \ totally\ \ in\ \ VL \\ 0, if\ \ pl\ \ is\ \ not\ \ in\ \ VL \\ > 0\ and < 1, if\ \ pl\ \ is\ \ partly\ \ in\ \ VL \end{cases} \cdots\cdots\cdots \tag{2}$$

If we use fuzzy sets, we can create overlapping functions to describe the membership sets to which an object can belong. In the case of vulnerability likelihood, we could use five membership sets (or classes) and then overlap very unlikely with unlikely, unlikely with possible, possible with likely and likely with very likely. The degree of membership of a particular object to a particular class will be defined by the mathematical function that describes the membership sets. The selection of an appropriate membership function is dependent on several factors, including appropriateness for the problem domain, ease of implementation and computational efficiency [31]. The use of overlapping sets enables fuzzy logic to deal with imprecision and subjectivity in a way that traditional set theory cannot. This makes it suited to problems where the expression of expertise can be imprecise and expressed in graduations, such as in a qualitative vulnerability prediction likelihood scale.

The methodology adopted followed three stages as described in Fig. 1. The first stage involved selecting the relevant vulnerability factors for use as system inputs and defining the system's outputs. The second stage followed the typical workflow of FIS development using the MATLAB fuzzy logic toolbox [32]. The final stage, once the operation of the prototype was confirmed as correct was the implementation of a software application that provided the functionality of the FIS for use by cybersecurity practitioners.

Fig. 2 provides greater detail of the stages undertaken, particularly concerning the development of the FIS. The expertise and supporting data used in this study were provided by two radio frequency (RF) engineer team leaders, from two independent organizations. Using the expertise from two different organisations provided improved coverage of the use case requirements needed to design and develop the FIS. The RF experts had a combined level of experience of more than 30 years, during which they applied their RF engineering skills to TEMPEST-related problems.

2.1. Fuzzy inference system input factors

Previous research had identified and modelled nineteen causal factors that RF engineers consider when assessing unintentional electromagnetic emanation vulnerabilities from office-based (thin client workstations) ITE [30]. Table 1 lists the identified vulnerability factors.

The FIS developed in this paper predicts the vulnerability likelihood before any mitigations are applied and therefore only requires a subset of these factors as input. The RF experts identified five categories: physical and supply chain security, ITE radiation distance, distance from the ITE and the secure perimeter, size of the installation, and utility lines leaving the secure perimeter. The relevant vulnerability factors from the original study were mapped into these categories as shown in Table 2.

The FIS aims to use these input measures to provide two qualitative output vulnerability likelihood levels (before any countermeasures are applied). One for the radiated vulnerability likelihood level and the other for the conducted vulnerability likelihood level.

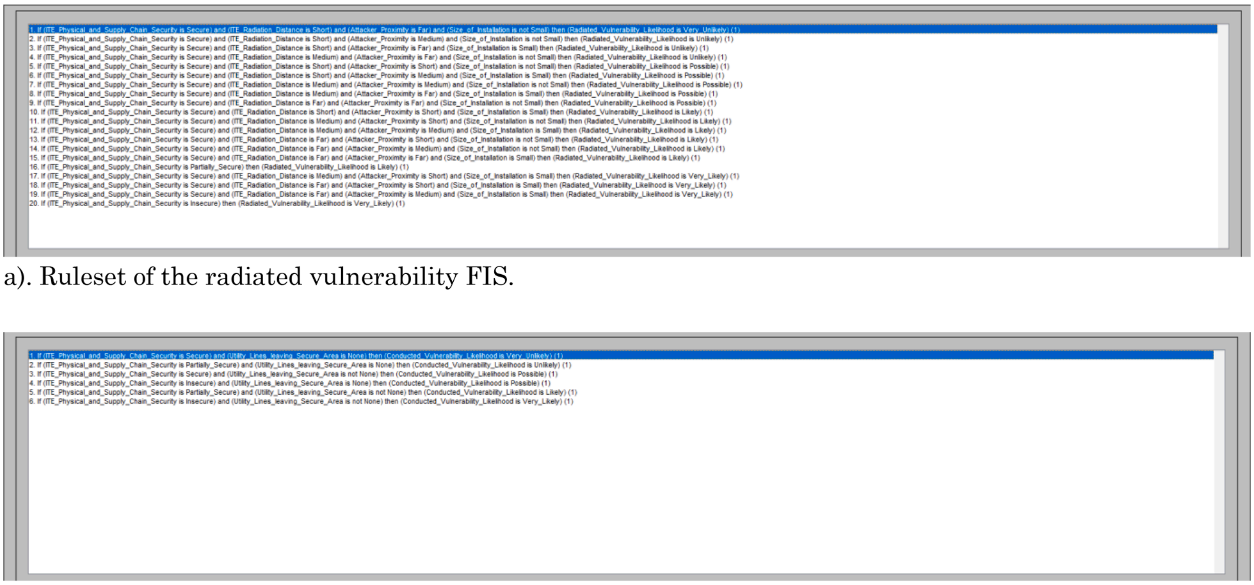
2.2. Fuzzy inference system development

Developing a FIS is a three-stage process, consisting of fuzzification, inference and defuzzification as shown in Fig. 3.

2.2.1. Fuzzification

Each of the five inputs and two outputs of the FIS was fuzzified by being divided into attributes (termed linguistic variables). Linguistic variables enable the articulation of qualitative quantities that are meaningful to humans when they describe things. In this model, each of the inputs has three linguistic variables, each described by a fuzzy membership function. The membership function describes the distribution of the linguistic variable $\mu_A(x)$ across the input range of values (x). The triangular and trapezoidal functions shown in Fig. 4 and described by Eqs. (3) and (4) were selected to describe set membership, as they are simple to implement and computationally fast [31].

Triangular membership function



```
1. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Far) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Very_Unlikely) (1)
2. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Medium) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Unlikely) (1)
3. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Far) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Unlikely) (1)
4. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Far) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Unlikely) (1)
5. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Short) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Possible) (1)
6. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Medium) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Possible) (1)
7. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Medium) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Possible) (1)
8. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Far) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Possible) (1)
9. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Far) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Possible) (1)
10. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Short) and (Attacker_Proximity is Short) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
11. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Short) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
12. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Medium) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
13. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Short) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
14. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Medium) and (Size_of_Installation is not Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
15. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Far) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Likely) (1)
16. If (ITE_Physical_and_Supply_Chain_Security is Partially_Secure) then (Radiated_Vulnerability_Likelihood is Likely) (1)
17. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Medium) and (Attacker_Proximity is Short) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Very_Likely) (1)
18. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Short) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Very_Likely) (1)
19. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (ITE_Radiation_Distance is Far) and (Attacker_Proximity is Medium) and (Size_of_Installation is Small) then (Radiated_Vulnerability_Likelihood is Very_Likely) (1)
20. If (ITE_Physical_and_Supply_Chain_Security is Insecure) then (Radiated_Vulnerability_Likelihood is Very_Likely) (1)
```

a). Ruleset of the radiated vulnerability FIS.

```
1. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (Utility_Lines_leaving_Secure_Area is None) then (Conducted_Vulnerability_Likelihood is Very_Unlikely) (1)
2. If (ITE_Physical_and_Supply_Chain_Security is Partially_Secure) and (Utility_Lines_leaving_Secure_Area is None) then (Conducted_Vulnerability_Likelihood is Unlikely) (1)
3. If (ITE_Physical_and_Supply_Chain_Security is Secure) and (Utility_Lines_leaving_Secure_Area is not None) then (Conducted_Vulnerability_Likelihood is Possible) (1)
4. If (ITE_Physical_and_Supply_Chain_Security is Insecure) and (Utility_Lines_leaving_Secure_Area is None) then (Conducted_Vulnerability_Likelihood is Possible) (1)
5. If (ITE_Physical_and_Supply_Chain_Security is Partially_Secure) and (Utility_Lines_leaving_Secure_Area is not None) then (Conducted_Vulnerability_Likelihood is Likely) (1)
6. If (ITE_Physical_and_Supply_Chain_Security is Insecure) and (Utility_Lines_leaving_Secure_Area is not None) then (Conducted_Vulnerability_Likelihood is Very_Likely) (1)
```

b). Ruleset of the conducted vulnerability FIS.

Fig. 8. FIS rulesets.

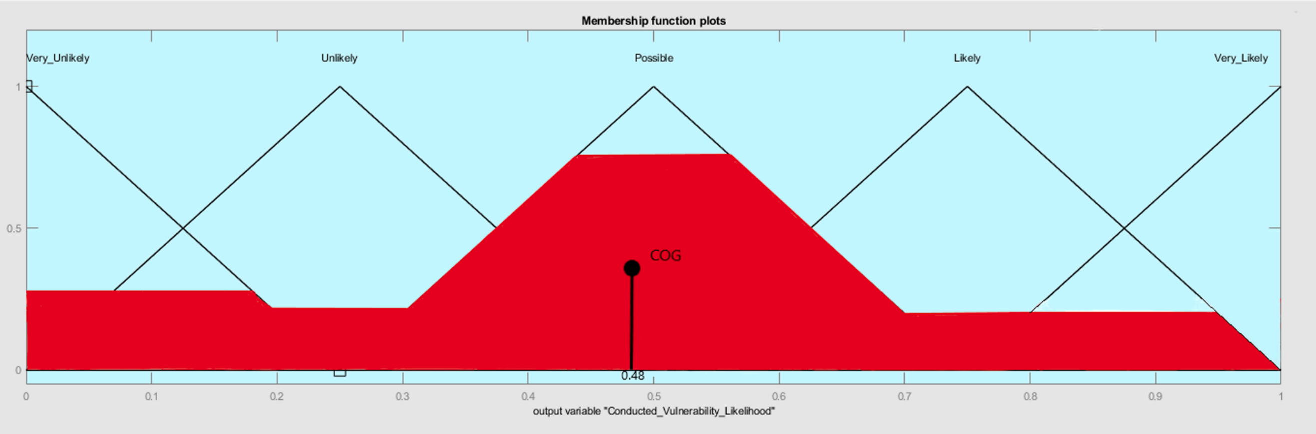


Fig. 9. Defuzzified output derived from the centroid function for the conducted vulnerability likelihood.

$$\mu_A(x;a,b,c) = \begin{cases} 0, x \le a \\ \dfrac{x-a}{b-a}, a \le x \le b \\ \dfrac{c-x}{c-b}, b \le x \le c \\ 0, c \le x \end{cases} \quad \cdots\cdots\cdots \tag{3}$$

Trapezoidal membership function

$$\mu_A(x;a,b,c,d) = \begin{cases} 0, x \le a \\ \dfrac{x-a}{b-a}, a \le x \le b \\ 1, b \le x \le c \\ \dfrac{d-x}{d-c}, c \le x \le d \\ 0, d \le x \end{cases} \quad \cdots\cdots\cdots \tag{4}$$

The range and fuzzy membership set for each of the FIS inputs and outputs are given in Table 3. As all five inputs have three membership sets, these combine to produce $3^5 = 243$ outcomes. These outcomes need to be accommodated by the fuzzy rules so that the correct output can be inferred from the presented inputs as part of the inference stage of the process.

It proved possible to reduce the number of outcomes by considering the relationship of the inputs to the outputs. In the case of I1, the lack of physical and supply chain security impacts both the radiated and conducted vulnerability outputs, as the equipment could be tampered with to create either of these vulnerabilities. How far equipment radiates (I2) is related to the radiated vulnerability likelihood. When a radiated emanation is fortuitously conducted onto a signal or power cable, a conducted vulnerability could occur. However, it would only be exploited if the utility cable were to leave the secure perimeter. Therefore, the distance between the ITE and the cable that could be used to conduct the transmission is less important from a conducted vulnerability perspective than whether the cable left the secure perimeter (I5) when the vulnerability could be exposed to attack. How close an attacker can get to the installation (I3) is very significant from a radiated vulnerability perspective. Radiated emissions are significantly attenuated as the distance increases due to path losses and local signal-to-noise conditions [33]. This means an attacker needs to get as close as possible to maximise their chance of successfully capturing any emanations. Conducted vulnerabilities can be exploited over considerable distances

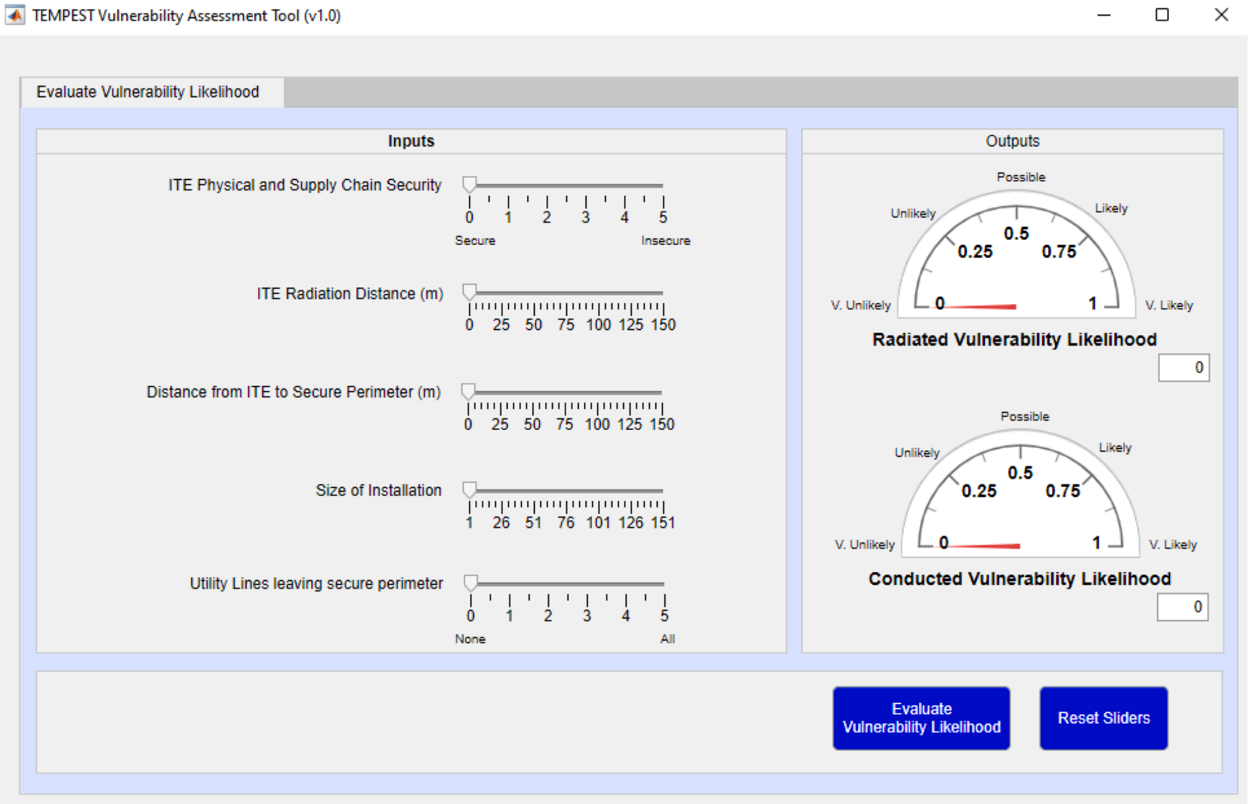

TEMPEST Vulnerability Assessment Tool (v1.0)
Evaluate Vulnerability Likelihood
Inputs
ITE Physical and Supply Chain Security
0 1 2 3 4 5
Secure
Insecure
ITE Radiation Distance (m)
0 25 50 75 100 125 150
Distance from ITE to Secure Perimeter (m)
0 25 50 75 100 125 150
Size of Installation
1 26 51 76 101 126 151
Utility Lines leaving secure perimeter
0 1 2 3 4 5
None
All
Outputs
Possible
Unlikely
Likely
0.5
0.25
0.75
V. Unlikely
0
1
V. Likely
Radiated Vulnerability Likelihood
0
Possible
Unlikely
Likely
0.5
0.25
0.75
V. Unlikely
0
1
V. Likely
Conducted Vulnerability Likelihood
0
Evaluate Vulnerability Likelihood
Reset Sliders

Fig. 10. MATLAB Program GUI.

[7]. However, this is dependent on whether cables that could be exhibiting these vulnerabilities are leaving the secure perimeter or not (I5). The size of the installation (I4) has significance for both radiated and conducted vulnerabilities. The larger the installation the greater the power consumption which will add to the facility's total power consumption affecting whether countermeasures post the vulnerability assessment will be necessary. As an installation will typically have its cable connections aggregated before interfacing with other networks and services e.g., through routers for internet access and through on-site transformers and sub-stations for power, the size of the installation is less significant than whether the aggregated cable connections are leaving the secure perimeter. Therefore, in terms of an initial vulnerability likelihood assessment, I4 will have more significance for radiated vulnerabilities than for conducted ones, as a large installation may create a noisy RF environment, making it difficult for attackers to target specific ITE and capture radiated emissions.

From these deliberations, it was possible to split the FIS into two separate systems, shown in Fig. 5, one to predict the radiated vulnerability likelihood using inputs I1 to I4, and the other to predict the conducted vulnerability likelihood using inputs I1 and I5. This in turn reduced the number of outcomes to $3^4 + 3^2 = 90$.

The RF experts were engaged to establish the membership sets for the inputs and outputs of both the radiated and conducted vulnerability FIS. E.g., for the ITE radiation distance input they agreed that a short distance was less than 20 m, a medium distance lay between 10 m and 100 m, and a far distance was greater than 90 m. Armed with this information it was possible to establish three membership sets (short, medium, and far) for this input using a trapezoidal shape. This approach was repeated for all inputs and outputs that were entered into the MATLAB fuzzy logic toolbox as shown in Fig. 6.

The process of fuzzification of the I1 and I5 input variables when the user is wanting a prediction of conducted vulnerability likelihood, is shown in Fig. 7. The input values are mapped onto the fuzzy membership sets for each of the linguistic variables to indicate the degree of membership. These values are the fuzzified input values which are used in the inference stage of the process.

In the case of I1, a value of 1.1 is shown mapped to 0.8 of the 'secure' membership set, 0.2 of the 'partially secure' membership set and 0 of the 'insecure' membership set. This produces a fuzzy variable for this input as [0.8,0.2,0]. In the case of I5, an input value of 0.75 is shown mapped to 0.25 of the 'none' membership set, 0.75 of the 'some' membership set and 0 of the 'all' membership set. Therefore, the fuzzy variable for this input is [0.25,0.75,0].

2.2.2. Fuzzy inference

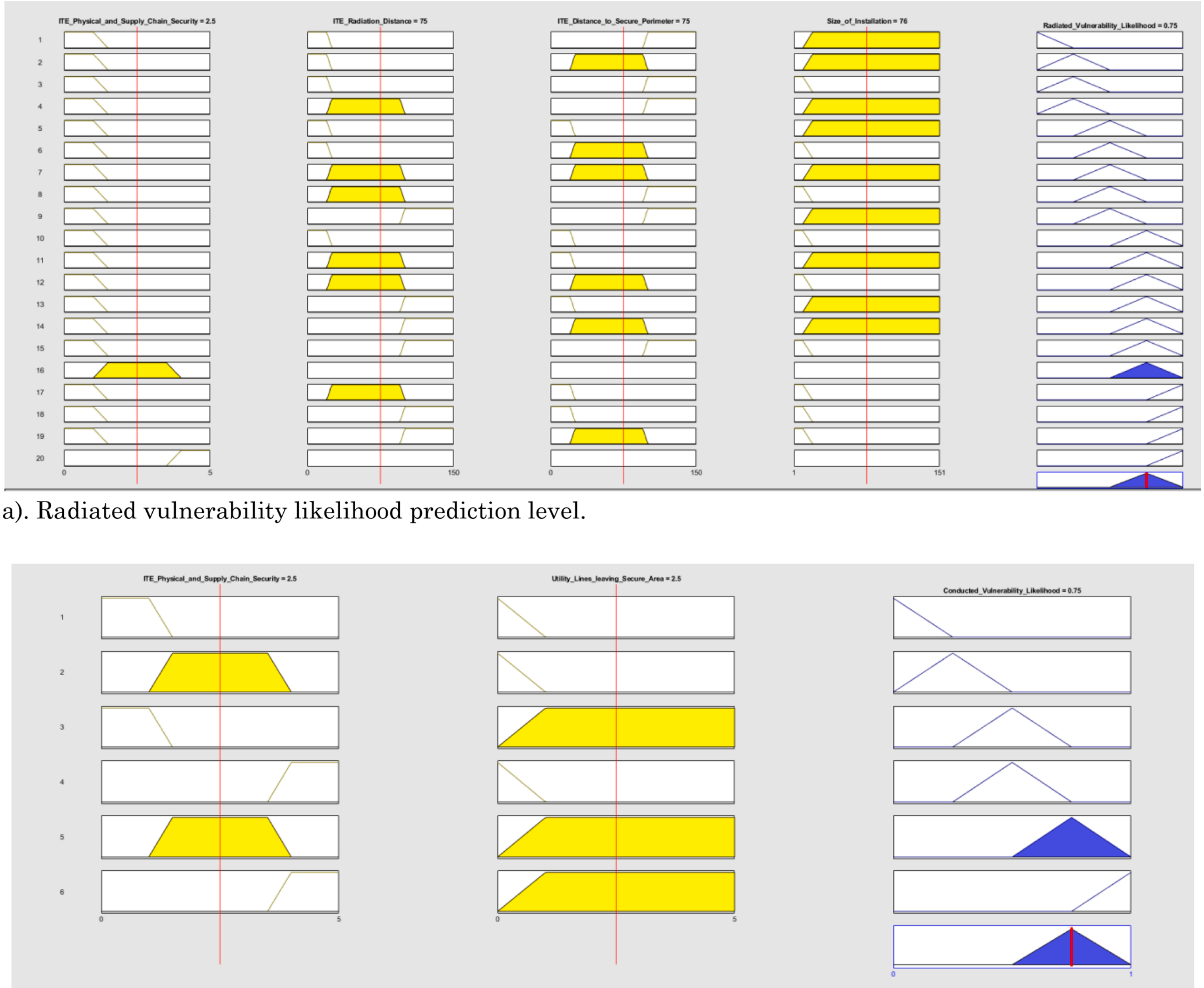
Inference is the stage of the process where the fuzzified input variables are applied to a set of fuzzy IF-THEN rules that codify the RF expert's knowledge. Mamdani modelling was used to derive the output membership functions for each rule to enable fuzzy decisions to be made. The Mamdani model was chosen as it is well suited to problems of this type where a decision or prediction must be made [21].

In the case of the radiated vulnerability FIS, it has 81 outcomes that were captured by a set of 20 rules developed with the RF experts. These are shown in Table 4.

The conducted vulnerability FIS has nine outcomes captured by six rules, shown in Table 5.

The rules for the radiated and conducted FIS' were then entered into the MATLAB fuzzy logic toolbox as shown in Fig. 8.

The inference process using the radiated and conducted vulnerability rulesets, along with the fuzzy variables for I1 to I5 will determine how much each rule affects the final outputs. Where the rule contains the AND function, the minimum value of the fuzzy variables will be used and where the rule contains the OR function the maximum value will be used. In the case of the conducted vulnerability likelihood prediction using the I1 and I5 fuzzy variables of [0.8, 0.2, 0] and [0.25, 0.75, 0] respectively, we can see that rule three affects the output prediction the most.



a). Radiated vulnerability likelihood prediction level.

b). Conducted vulnerability likelihood prediction level.

Fig. 11. FIS performance analysis.

Rule 1: Very Unlikely = Min(I1 = secure, I5 = none) = Min(0.8, 0.25) = 0.25
Rule 2: Unlikely = Min(I1 = partially secure, I5 = none) = Min(0.2, 0.25) = 0.2
Rule 3: Possible = Min(I1 = secure, I5 = not none) = Min(0.8, 0.75) = 0.75
Rule 4: Possible = Min(I1 = insecure, I5 = none) = Min(0, 0.25) = 0
Rule 5: Likely = Min(I1 = partially secure, I5 = not none) = Min (0.2,0.75) = 0.2
Rule 6: Very Likely = Min(I1 = insecure, I5 = not none) = Min (0,0.75) = 0

2.2.3. Defuzzification

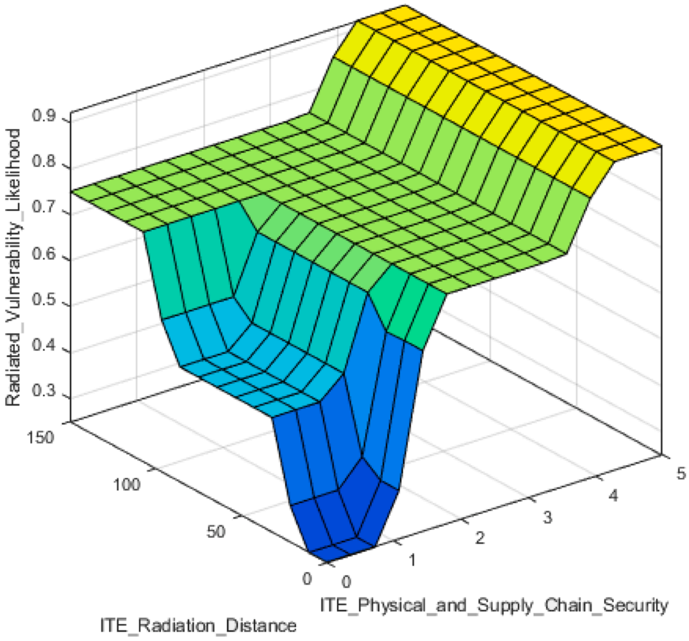
The fuzzy outputs of the radiated and conducted vulnerability FIS' must be defuzzified. Each fuzzy output variable is applied to its output membership sets and aggregated to derive the likelihood predictions for the radiated and conducted vulnerabilities. The centroid function, given by Eq. (5), is commonly used in applications of this type to find the centre of gravity (COG) of the aggregated shape. The COG for the two-dimensional shape will have an (x,y) coordinate. The x coordinate divides the aggregated shape into two equal masses.

$$xCentroid = \frac{\sum_i \mu(x_i)x_i}{\sum_i \mu(x_i)}\dots\dots\dots \tag{5}$$

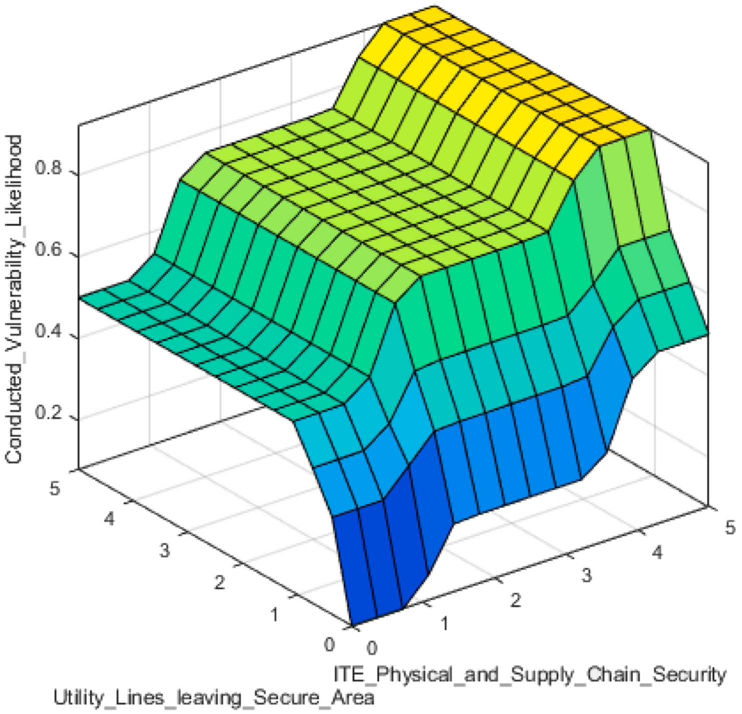
Fig. 9 shows graphically how the conducted vulnerability likelihood prediction is derived from this aggregation, with the centre of the resulting shape (along the x-axis) giving a crisp output value of 0.48 for the conducted vulnerability likelihood prediction.

2.3. Implementing the Fuzzy Inference System

As described in Sections 2.1 and 2.2 the combination of FIS inputs leads to 90 expected outcomes, as articulated by the RF experts. The FIS' radiated and conducted vulnerability likelihood predictions were tabulated and tested against these outcomes. Additionally, the RF experts presented input values with vulnerability predictions for 15 real-world use cases based on their experience in the field. These covered a range of scenarios from small to large installations occupying single buildings and sites, to shared occupancy buildings and sites, with different operational challenges such as reduced perimeter distances. These were also tabulated along with the FIS' predictions of vulnerability likelihood for each of the use case scenarios.



a). Surface view of radiated vulnerability likelihood output.



b). Surface view of the conducted vulnerability likelihood output.

Fig. 12. Surface view of FIS performance analysis.

2.3.1. MATLAB application

The MATLAB fuzzy logic toolbox was used to prototype the radiated and conducted FIS' separately. As the overall FIS needs to integrate these, a program was written using MATLAB application designer which enabled a graphical user interface (GUI) to be added. This made working with the RF experts easier when optimising the functionality of the program and when assessing its performance. The GUI version would also be released to cyber security practitioners to enable them to assess the vulnerability likelihood. Fig. 10 shows the GUI of the MATLAB program.

To provide an assessment of the radiated vulnerability likelihood level for the scenario being addressed, the user is asked to provide a judgement on their perception of the physical and supply chain security of the ITE. They enter a value of between zero to five, representing their assessment from secure to insecure, using the slider control provided. They are then asked to provide a value for the ITE radiation distance,

Table 6
FIS output thresholds.

Output Value	Threshold
Very Unlikely	<=0.125
Unlikely	>0.125 - <=0.375
Possible	>0.375 - <=0.625
Likely	>0.625 - <=0.875
Very Likely	>0.875

using the slider control. This value is dependent on the ITE type and its installation. Typically, if the ITE and its connections are shielded then the radiation distance is less than 20 m. If the ITE and its connections are unshielded, then distances more than 100 m are possible. Where the installation has a mixture of shielded and unshielded ITE and connections then the distance will typically lie within the range 20 m to 100 m. The user then provides a measure of the distance from the ITE to the secure perimeter boundary, using the slider control provided. The relationship between the ITE radiation distance and the distance from the ITE to the secure boundary governs the radiated vulnerability likelihood, in that if the ITE radiates within the secure boundary but no further, then provided physical and supply chain security is robust there is less likelihood of a radiated vulnerability occurring. The user then enters a value for the number of ITEs ranging from 1 unit to 150 units, covering the range from a small installation to a large one. This input, along with the previous three are used to evaluate the radiated vulnerability likelihood level. This is displayed as a number in the range zero to one by a semi-circular gauge covering the range of very unlikely to very likely.

To provide an assessment of the conducted vulnerability likelihood level, the user is asked to confirm whether any utility i.e., signal or power lines are leaving the secure perimeter, by entering a value of between zero and five using the slider control provided. The answer will be used with their response to the physical and supply chain security input, to evaluate the conducted vulnerability likelihood level. This is displayed in the same manner for the radiated vulnerability likelihood level, as a number in the range zero to one, shown on a semi-circular gauge covering the range very unlikely to very likely.

3. Results

The performance of the fuzzy inference system (FIS) to predict the vulnerability likelihood levels were obtained from the defuzzified output values of the radiated and conducted FIS' as shown in Fig. 11. The input values are shown in yellow and the output values are in blue.

Fig. 12 shows the surface view of the performance analysis, where the input values are mapped against the output values. In the case of the radiated vulnerability likelihood (Fig. 12a) we can see that the likelihood increases as expected when the physical and supply chain security degrades or when the ITE radiates over greater distances. Similarly, for the conducted vulnerability likelihood (Fig. 12b), we see an increase in likelihood when the physical and supply chain security degrades, and utility lines are leaving the secure perimeter.

The FIS outputs for the prediction of the radiated and conducted vulnerability occupy the range of zero to one. This range was subdivided into five bands (shown in Table 6) to enable the crisp output prediction to be compared with the qualitative assessment made by the radio frequency (RF) experts.

The FIS was optimised against the 90 outcomes and its results compared to those expected by the RF experts. Where the outputs deviated from the expert's view the membership and rule sets were modified until the FIS outputs aligned with the RF experts' predictions. A sample of the optimisation matrix is shown in Table 7.

The FIS was then tested against a set of real-world use cases developed by the RF experts. The results are given in Table 8 and show that the FIS outcomes completely align with the experts' predictions showing a 100% success rate.

4. Discussion

This study has shown how a TEMPEST vulnerability prediction model was developed with the assistance of radio frequency (RF) engineering expertise, from two different organisations, using a fuzzy logic approach. The resulting fuzzy inference system (FIS) can be used by cyber security practitioners without RF expertise to make a vulnerability likelihood prediction. This has the potential of saving time and money, by enabling early decisions around the level of potential mitigations required. Fuzzy logic was chosen because it enables ambiguity and imprecision to be dealt with when accommodating the elicitation of expertise from humans. It is the authors' belief, that this is the first attempt at producing a prediction model for these types of vulnerabilities that could be used by non-RF experts.

Cyber security risk managers and associated professionals are tasked with assessing and managing cyber and information-related risks, including those from unintentional emanations. Managing risks of this

Table 7
Sample of the optimisation Test Matrix.

Input Conditions						Output Conditions			
Outcome	I1	I2	I3	I4	I5	O1 Expected	O1 Actual	O2 Expected	O2 Actual
8	Secure (1.0)	Short (10 m)	Far (120 m)	Medium (75)	–	Very Unlikely (<=0.125)	0.08	–	–
17	Secure (1.0)	Medium (60 m)	Far (120 m)	Medium (75)	–	Unlikely (>0.125 - <=0.375)	0.25	–	–
27	Secure (1.0)	Far (120 m)	Far (120 m)	Large (125)	–	Possible (>0.375 - <=0.625)	0.5	–	–
28	Partially Secure (3.0)	Short (10 m)	Short (10 m)	Small (5)	–	Likely (>0.625 - <=0.875)	0.75	–	–
55	Insecure (4.0)	Short (10 m)	Short (10 m)	Small (5)	–	Very Likely (>0.875)	0.92	–	–
82	Secure (1.0)	–	–	–	None (0)	–	–	Very Unlikely (<=0.125)	0.08
83	Secure (1.0)	–	–	–	Some (3.0)	–	–	Possible (>0.375 – <=0.625)	0.5
85	Partially Secure (3.0)	–	–	–	None (0)	–	–	Unlikely (>0.125 - <=0.375)	0.25
86	Partially Secure (3.0)	–	–	–	Some (3.0)	–	–	Likely (>0.625 - <=0.875)	0.75
90	Insecure (5.0)	–	–	–	All (5.0)	–	–	Very Likely (>0.875)	0.92

Table 8
FIS Test Results for the real-world use cases.

	Use Cases														
Input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
I1	0.5	1	1	1	1	2	4	2	1	1	2	1	1	1.5	0
I2	102 *m*	105 *m*	30 *m*	110 *m*	35 *m*	25 *m*	115 *m*	60 *m*	1 *m*	75 *m*	35 *m*	60 *m*	20 *m*	70 *m*	27 *m*
I3	87 *m*	5 *m*	10 *m*	5 *m*	100 *m*	7 *m*	1 *m*	9 *m*	12 *m*	2 *m*	3 *m*	>150 *m*	100 *m*	100 *m*	>150 *m*
I4	46	101	5	36	11	20	1	50	10	3	26	14	>151	6	1
I5	1	5	5	5	4	5	2	3	5	5	5	0	3	5	5
O1: Expected	Likely (>0.625 - <=0.875)	Likely (>0.625 - <=0.875)	Very Likely (>0.875)	Likely (>0.625 - <=0.875)	Possible (>0.375 -<=0.625)	Likely (>0.625 - <=0.875)	Very Likely (>0.875)	Likely (>0.625 - <=0.875)	Likely (>0.625 - <=0.875)	Very Likely (>0.875)	Likely (>0.625 - <=0.875)	Unlikely >0.125 - <=0.375	Very Unlikely <=0.125	Likely (>0.625 - <=0.875)	Possible (>0.375 - <=0.625)
O1: Actual	0.67	0.75	0.92	0.75	0.5	0.75	0.92	0.75	0.72	0.92	0.75	0.354	0.08	0.75	0.42
O2: Expected	Possible (>0.375 -<=0.625)	Possible (>0.375 -<=0.625)	Possible (>0.375 -<=0.625)	Possible (>0.375 -<=0.625)	Possible (>0.375 -<=0.625)	Likely (>0.625 - <=0.875)	Very Likely (>0.875)	Likely (>0.625 - <=0.875)	Possible (>0.375 -<=0.625)	Possible (>0.375 -<=0.625)	Likely (>0.625 - <=0.875)	Very Unlikely <=0.125	Possible (>0.375 -<=0.625)	Likely (>0.625 - <=0.875)	Possible (>0.375 -<=0.625)
O2: Actual	0.5	0.5	0.5	0.5	0.5	0.75	0.92	0.75	0.5	0.5	0.75	0.08	0.5	0.75	0.5

type requires specialist knowledge provided by RF engineering consultancy services [14] which can be resource intensive, requiring assistance with risk assessment, site visits, equipment evaluation, and testing. TEMPEST and unintentional emanation risks are now included in security management frameworks such as those advocated by the ISO 27000 series of standards and specifically ISO 27005 [13]. The detail that explains these vulnerabilities and mitigation measures is not always sufficient and requires cyber security practitioners to either examine the research papers or available TEMPEST documentation and/or use RF consultancy services. Additionally, experts and novices with different levels of prior knowledge relating to a specific domain will tend to use different approaches when processing information [34]. This may extend to cyber security practitioners without prior knowledge of electromagnetic-related vulnerabilities who may not give the same consideration to the risk that can result from these types of vulnerabilities. Therefore, by enabling non-RF experts to predict the likelihood of unintentional emanations occurring, using a prediction model and associated tool that encapsulates the RF expertise, makes risk management timelier and more cost-effective. This is achieved by reducing the dependency on potentially expensive and scarce RF consultancy services.

The prediction model developed in this study used five inputs, four to predict the radiated vulnerability likelihood and two to predict the conducted vulnerability likelihood. The radiated likelihood prediction relies on a user of the model being able to assess physical and supply chain security, the distance the information technology equipment (ITE) will radiate, the distance from the ITE to the secure perimeter and the number of ITEs in the installation. Physical security and distance of ITE to the secure perimeter can be assessed from a physical inspection, checking out the guard and access control arrangements e.g., guards with swipe access to rooms etc. and measuring distances. Supply chain integrity can be confirmed by checking that appropriate manufacturing, procurement and maintenance arrangements are in place. The number of ITE in an installation can be counted. The input that is most difficult to assess is how far will an ITE radiate. A definite answer to this question is only possible through testing, which when making the initial vulnerability assessment is not practicable. Therefore, the question arises how best to estimate this distance. Typically, there are two aspects to consider. What type of equipment is the ITE making up the installation and how is it connected? E.g., if the equipment is shielded (that is, has a TEMPEST certification) and is installed using the appropriate fibre or shielded cables then the distance will be possible to specify according to the certification. Where the installation is made from uncertified TEMPEST ITE with unshielded cables then the estimation of greater than 100m may be appropriate. If the installation uses a mix of shielded and unshielded ITE and cable connections, then a radiation distance of between 20m and 100m could be assumed. Alternatively, the practitioner using the prediction model may decide on a distance based on prior knowledge of a particular ITE manufacturer or use a prediction based on the maximum radiation distance taking the electromagnetic compatibility results into account [35].

It is worth noting that the prediction model's rules are based on the ranges of the fuzzy membership sets. When the ITE radiation distance is compared with the distance of the ITE to the secure perimeter, what matters is whether the radiation distances specified for these two inputs lie in the same range, and not the difference between them. E.g., if the ITE radiation distance is 70m (lying in the range of 20m to 100m) and the distance from the ITE to the secure perimeter is 50m (also in the same range) the fuzzy model will predict a vulnerability likelihood on the basis they both covering the same medium distance. Given that estimating the ITE radiation distance is based on the ITE type and connection, there is the potential to improve the model by asking the user to enter these details from which the model makes the distance estimate, rather than asking for a specific distance. Though some flexibility would be lost if the user had some prior knowledge of the ITE and its radiation profile.

In the case of the conducted vulnerability likelihood prediction, the user is asked to assess physical and supply chain security as for the radiated vulnerability case. They are also asked if any of the utility (signal and power) connections leave the secure perimeter. The membership sets agreed for this input declared no lines, some lines or all lines leave the secure perimeter. In practice, the level of assessed conducted vulnerability as specified by the expert fuzzy rules, does not make any distinction between some or all lines leaving the secure perimeter. This offers a potential improvement of the model where only two memberships are required for this input with the potential to make this a binary yes/no decision.

Considerable time was spent with the experts to optimise the performance of the system for all 90 outcomes of the five input FIS. By ensuring that these results were correct, the expectation that the real-world test case predictions would also be correct was proven, with all fifteen case predictions aligning with those of the RF experts. Future work will extend the model to include propagation effects and countermeasures. This will enable the prediction model to present both a pre-mitigation and post-mitigation vulnerability likelihood level.

5. Conclusions

The output from this study demonstrates that fuzzy logic can be used to build a fuzzy inference system (FIS) capable of providing a TEMPEST radiated and conducted vulnerability likelihood prediction for office-based information technology equipment. The study has employed radio frequency (RF) expertise from two independent organisations to develop the fuzzy membership sets and associated fuzzy rule base. The FIS has successfully predicted the correct level of radiated and conducted vulnerability likelihood for the most prevalent scenarios dealt with by the RF experts. This enables the FIS to be used by cybersecurity practitioners who do not possess RF expertise but are tasked with assessing risks from TEMPEST vulnerabilities. The model and associated tool have the potential to save time and money by removing the dependence on RF consultancy services, particularly at the initial stages of a project before mitigation measures have been decided. Future work will include extending the FIS to include RF propagation models and a vulnerability likelihood prediction after countermeasures have been applied.

The authors would like to thank the RF engineering team leaders from the National Cyber Security Centre (NCSC) and the UK National Authority for Counter Eavesdropping (NACE), as without their support this study would not have been possible.

Declaration of Competing Interest

The 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] 'Electromagnetic Compatibility'. http://www.bsigroup.com/en-GB/industries-and-sectors/electrical-and-electronic/electromagnetic-compatibility/ (accessed Sep. 02, 2022).

[2] W. M. NSA, 'TEMPEST: A Signal Problem', Sep. 18, 2013. https://web.archive.org/web/20130918021523/http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf (accessed Feb. 11, 2022).

[3] W. van Eck, Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Comput. Secur. 4 (1985) 269–286.

[4] M.G. Kuhn, Electromagnetic Eavesdropping Risks of Flat-Panel Displays, in: Privacy Enhancing Technologies, D. Martin and A. Serjantov, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2005, pp. 88–107. doi: 10.1007/11423409_7.

[5] M. Vuagnoux, S. Pasini, Compromising electromagnetic emanations of wired and wireless keyboards, in: Proceedings of the 18th conference on USENIX security symposium, in SSYM'09. USA: USENIX Association, Aug. 2009, pp. 1–16.

[6] K.A. Ghani, K. Dimyati, K. Ismail, L.S. Supian, Radiated Emission from Handheld Devices with Touch-Screen LCDs, in: 2013 European Intelligence and Security Informatics Conference, Aug. 2013, pp. 219–219. doi: 10.1109/EISIC.2013.51.

[7] R. Gehling, C.R. Ashley, T. Griffin, Electronic Emissions Security: Danger in the Air, Inf. Syst. Manag. 24 (2007) 305–310, https://doi.org/10.1080/10580530701586011.

[8] A. Auddy, S. Sahu, 'Tempest: Magnitude of threat and mitigation techniques', in: 2008 10th International Conference on Electromagnetic Interference Compatibility, Nov. 2008, pp. 603–611.

[9] ApiTech, TEMPEST Introduction, ApiTech, 2021. https://www.apitech.com/brands/secure-systems-information-assurance/sst/what-is-tempest/ (accessed Jan. 09, 2021).

[10] Cisco, 'Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper', Cisco, Mar. 09, 2020. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed Jan. 06, 2021).

[11] P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, Med. Devices Auckl. NZ 8 (2015) 305–316, https://doi.org/10.2147/MDER.S50048.

[12] A. Souza, I. Carlson, H.S. Ramos, A.A.F. Loureiro, L.B. Oliveira, Internet of Things device authentication via electromagnetic fingerprints, Eng. Rep. 2 (8) (2020), e12226, https://doi.org/10.1002/eng2.12226.

[13] ISO/IEC, 'ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management'. International Standards Organisation (ISO), 2011.

[14] NCSC, 'TEMPEST and Electromagnetic Security', 2018. https://www.ncsc.gov.uk/information/tempest-and-electromagnetic-security (accessed Apr. 26, 2021).

[15] 'Rf Engineer Jobs, Careers & Recruitment - Updated Daily - totaljobs', totaljobs.com. https://www.totaljobs.com/jobs/rf-engineer (accessed May 14, 2023).

[16] 'Verify suppliers'. https://www.ncsc.gov.uk/section/products-services/verify-suppliers (accessed May 14, 2023).

[17] '28_05_2019_Full_Review_SOL_Final_Report_1159.pdf'. Accessed: May 14, 2023. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/806331/28_05_2019_Full_Review_SOL_Final_Report_1159.pdf.

[18] ISO/IEC, 'ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management'. International Standards Organisation (ISO), 2005.

[19] M.A. Williams, R.C. Barranco, S.M. Naim, S. Dey, M. Shahriar Hossain, M. Akbar, A vulnerability analysis and prediction framework, Comput. Secur. 92 (May 2020), 101751, https://doi.org/10.1016/j.cose.2020.101751.

[20] Needs and Importance of Reliability Prediction: An Industrial Perspective', Inf. Sci. Lett., 9(1) (2020) 33–37, doi: 10.18576/isl/090105.

[21] K. Sahu, F.A. Al-Zahrani, R.K. Srivastava, R. Kumar, Evaluating the Impact of Prediction Techniques: Software Reliability Perspective, Comput. Mater. Contin. 67 (Feb. 2021) 1471–1488, https://doi.org/10.32604/cmc.2021.014868.

[22] K. Sahu, R.K. Srivastava, Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: reliability perspective, Adv. Math. Sci. J. 10 (1) (Jan. 2021) 543–555, https://doi.org/10.37418/amsj.10.1.54.

[23] K.R. Chervinskaya, E.L. Wasserman, Some methodological aspects of tacit knowledge elicitation, J. Exp. Theor. Artif. Intell. 12 (1) (Jan. 2000) 43–55, https://doi.org/10.1080/095281300146308.

[24] L.A. Zadeh, Fuzzy sets, Inf. Control 8 (3) (Jun. 1965) 338–353, https://doi.org/10.1016/S0019-9958(65)90241-X.

[25] H. Singh, et al., Real-Life Applications of Fuzzy Logic, Adv. Fuzzy Syst. 2013 (Jun. 2013), e581879, https://doi.org/10.1155/2013/581879.

[26] A.C. Bukhari, I. Tusseyeva, B.-G. Lee, Y.-G. Kim, An intelligent real-time multi-vessel collision risk assessment system from VTS view point based on fuzzy inference system, Expert Syst. Appl. 40 (4) (2013) 1220–1230, https://doi.org/10.1016/j.eswa.2012.08.016.

[27] A.K. Lohani, N.K. Goel, K.K.S. Bhatia, Improving real time flood forecasting using fuzzy inference system, J. Hydrol. 509 (Feb. 2014) 25–41, https://doi.org/10.1016/j.jhydrol.2013.11.021.

[28] I.B. de Medeiros, M.A. Soares Machado, W.J. Damasceno, A.M. Caldeira, R.C. dos Santos, J.B. da Silva Filho, A Fuzzy Inference System to Support Medical Diagnosis in Real Time, Procedia Comput. Sci. 122 (Jan. 2017) 167–173, https://doi.org/10.1016/j.procs.2017.11.356.

[29] L. Jouffe, Fuzzy inference system learning by reinforcement methods, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 28 (3) (Aug. 1998) 338–355, https://doi.org/10.1109/5326.704563.

[30] M. Martin, F. Sunmola, and D. Lauder, 'Likelihood of Unintentional Electromagnetic Emanations Compromising IT Equipment Security: Perspectives of Practitioners on Causal Factors', in 2021 International Carnahan Conference on Security Technology (ICCST), Oct. 2021, pp. 1–6. doi: 10.1109/ICCST49569.2021.9717369.

[31] A. Sadollah, A. Sadollah, Introductory Chapter: Which Membership Function is Appropriate in Fuzzy System? IntechOpen (2018) https://doi.org/10.5772/intechopen.79552.

[32] 'Build Fuzzy Systems Using Fuzzy Logic Designer - MATLAB & Simulink - MathWorks United Kingdom'. https://uk.mathworks.com/help/fuzzy/building-systems-with-fuzzy-logic-toolbox-software.html (accessed May 22, 2023).

[33] L. Paunovska, L. Gavrilovska, 'Comparison of propagation models ITU.R-P.1546 and ITU.R-P.1812', in 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), May 2014, pp. 1–5. doi: 10.1109/VITAE.2014.6934481.

[34] S.Y. Chen, R. Macredie, Web-based interaction: A review of three important human factors, Int. J. Inf. Manag. 30 (5) (Oct. 2010) 379–387, https://doi.org/10.1016/j.ijinfomgt.2010.02.009.

[35] H. Sekiguchi, S. Seto, Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage, IEEE Trans. Electromagn. Compat. 55 (3) (Jun. 2013) 547–554, https://doi.org/10.1109/TEMC.2012.2232297.