IET Cyber-Physical Systems: Theory & Applications

Research Article

IET Journals
The Institution of Engineering and Technology

Assets focus risk management framework for critical infrastructure cybersecurity risk management

ISSN 2398-3396
Received on 23rd December 2018
Revised 24th April 2019
Accepted on 7th May 2019
E-First on 3rd June 2019
doi: 10.1049/iet-cps.2018.5079
www.ietdl.org

Halima Ibrahim Kure[1] ✉, *Shareeful Islam*[1]

[1]*School of Architecture, Computing, and Engineering, University of East London, London E162RD, UK*
✉ *E-mail: h.kure@uel.ac.uk*

Abstract: Critical infrastructure (CI) is vital for the overall economic growth and its reliable and safe operation is essential for a nation's stability and people's safety. Proper operation of the assets is essential for such a system and any threats that could negatively impact the asset could have a severe disruption. Risk management is an important aspect of the protection of CI. There are several frameworks and methodologies for identifying assets, quantifying and analysing vulnerabilities. However, there is a lack of focus on the interdependencies among the assets and cascading effect of the inherent vulnerabilities on the asset. This study attempts to bridge that gap by presenting a novel asset focus risk management approach for the CI. It presents a systematic methodology for identifying and analysing critical assets, their potential vulnerabilities, threats and risks facing CI. This work taking into account cascading vulnerability impacts on assets leading to threats and causing risk. The authors use a running example from a smart grid system to demonstrate the usability of the approach. The result shows that some assets are prioritised and more vulnerable than other assets for the power grid system and it can severely impact on the overall business continuity.

1 Introduction

Critical Infrastructure (CI) organisations comprise of critical assets such as information technology (IT) hardware, software, environmental, facilities, technology, networks, services, people and complex processes inter-related with other to support the overall business. Due to its inherent complex nature of technology and its interaction with people and systems consisting of multiple, distributed, and independently operating systems [1], it faces different security threats including cybersecurity threats, physical attack, etc. which could lead to any potential risks. Risks are associated with all aspects of CI, as it is the probability of loss [2] or an uncertain event that may occur and influence the organisation's achievement on strategic, operational, and financial objectives [3]. The cybersecurity threat is one of the most urgent issues in the CI organisation, its networks and associated assets and vulnerabilities [4]. It is necessary to identify the assets, prioritising them based on their dependencies to support the overall business so that adequate protection can be implemented to protect the assets. An effective risk management practice is necessary for this purpose. There are existing risk management methods and standards such as ISO 31000:2018 that embodies the identification, analysis, planning, tracking, controlling, and communication of risk which gives a structured mechanism to provide visibility of the risks in order to achieve the organisation's success [5]. However, there is a lack of focus on identifying and analysing cascading effects from vulnerability to threat and risks.

The novel contribution of this paper is an asset focus risk management framework that identifies the assets and their vulnerabilities and analyses possible vulnerabilities by showing their cascading effects on the assets and contribution to the threat and risks. We follow concepts relating to the asset, threat, and risks and use a systematic process to identify and prioritise the assets and vulnerabilities. The assets and risks are analysed through the cascading effect of vulnerabilities to the asset and cause the risks. This certainly helps the CI organisation to mitigate the vulnerabilities and risks by using suitable controls in a proactive way. We use a running example of a power grid system to demonstrate the applicability of the work. The results show that the proposed approach effectively identifies vulnerabilities of the assets and analyse the risks through the cascading influence of vulnerabilities on the assets.

2 Related work

There are works in literature that have been proposed on identifying assets, their potential vulnerabilities, possible threat outcomes, risk, and risk assessment but has not been systematically addressed. Izuakor and White [6] proposed a new approach for CI asset identification using multi-criteria decision theory to resolve the challenges of identifying critical assets. The approach did not provide a systematic process for arriving at a critical decision. Bialas [7] proposed a novel structured risk management approach on how to deal with internal and external impacts of a hazardous event which occurred in the given CI. It followed an ISO31000 standard of risk monitoring and risk communication. This paper additionally takes into account interdependencies. The paper did not provide a guideline for determining risk levels and control mitigations. Fekete [8] described how society gets to choose what is critical to them, based on how much influence it has on them. This shows how to identify what is critical with regard to the fact that there cannot be full protection with respect to cascading effects and threats. The paper focuses less on threat prevention rather than the impacts of threats. Strategic proactive planning, the purpose of civil protection and activities of risk management are among the key attributes of identifying the above. The authors in [9] analysed a telecommunication system by adopting unified modelling language (UML) to build a model named TVRA model for the telecommunication system which also made a systematic analysis about the security objectives, assets, weaknesses, unwanted incidents, threats. Clarizia *et al*.[10] proposed a multi-level graph approach that collects and analyses data from sensors within a city using context dimension tree, ontologies, and baysian belief networks for the purpose of decision-making. The underlying system architecture data collection, context, and interface engine. However, to improve its performance knowledge sharing and exchanging is important. Wang and Liu [11] extended in their work a new attribute 'location' and proposed a comprehensive vulnerability analysis model for internet protocol (IP) Multimedia Subsystem (IMS) network. They could identify weaknesses in the IMS system, therefore, making the system vulnerable, but did not

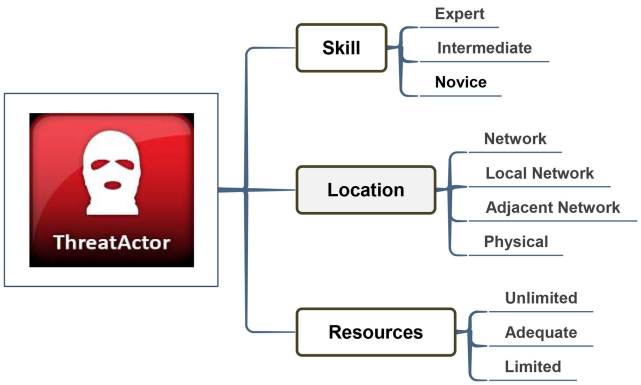

Fig. 1 *Threat actor profile*

focus on how to reduce those weaknesses. This new model also tried to focus on all the assets and treating them as equal. The asset identification aspect of this model did not identify the most critical assets of the system. Ramakrishnan and Sekar [12] proposed a novel technique to identify vulnerabilities that arise from unexpected interactions between system components. The behaviour of each system component is modelled in high-level specification language to obtain possible behaviours of an entire system. The behaviours are further analysed to find vulnerabilities within the system by using automated verification techniques to identify scenarios where security-related properties are violated. Ezell [13] presented a model that quantifies vulnerability by using the Infrastructure Vulnerability Assessment Model and applied it to a medium-sized clean water system. This paper did not identify assets but rather quantified vulnerabilities of the overall system. Cherdantseva [14] reviewed the state of the art in cybersecurity risk assessment of the supervisory control and data acquisition (SCADA) systems. In the work, many risk assessment methods developed or applied in the context of a SCADA system were examined. These various methods were analysed in terms of aim, application domain, stages of risk management, risk management concepts, impact measurement, and sources of probabilistic data, evaluation and tool support. Based on the analysis of an intuitive scheme for the categorisation of cybersecurity risk assessment methods for SCADA systems was suggested.

McQueen *et al*. [15] proposed a model for estimating the time to compromise a system component that is visible to an attacker. The model provides an estimate of the expected value of the time-to-compromise as a function of known and visible vulnerabilities, and attacker skill level. The model was used to aid in risk reduction estimate between a SCADA system and baseline system. In the work of McQueen *et al*. [16], risk reduction on a partial SCADA system was carried out and a methodology was developed for obtaining quantitative risk reduction estimation. The methodology applied a graph theoretical approach which was described in ten steps. McQueen *et al*. [15] discussed the specific methods used in step six of the methodology, estimating the time-to-compromise. There are standards such as the North American Electric Reliability Corporation (NERC) established the cybersecurity standards for CI protection (CIP-002 through CIP 009) to provide a security framework for the identification and protection of critical cyber assets that support the reliable operation of the electric power grid [17]. National Institute of standards and technology (NIST) developed the cybersecurity framework to enhance the security and resilience of a nations CI [18]. NIST provides a risk management framework to improve information security, strengthen risk management processes, and encourage its adoption among organisations.

All these works justify the necessity and importance of identifying critical assets and vulnerabilities of the assets of CI. However, we have made several observations. In particular, there is a lack of systematic approach that supports CI organisation by identifying critical assets and their vulnerabilities and cascading effect of the vulnerabilities on the assets. Furthermore, most of the risk management process emphasises more on vulnerability assessment for CI rather than on identifying critical assets before assessing vulnerability. The novel contribution of our work is a systematic asset identification and vulnerability assessment approach for CI risk management taking into account the cascading effect of vulnerability on the threat and risk.

3 Running example

This section provides an overview of the running example power grid SCADA system used by our work. The system is composed of three main components, i.e. power plant, transmission substation, and distribution grid. The power grid is a network of power lines and associated equipment used to transmit and distribute electricity over a geographic area. Such facilities include transportation, communication systems, water, electricity, and public institutions like schools, hospitals, post offices, and even prisons [19]. The cyber-physical systems of the electric sector include industrial control systems (ICS), which allow digital control of the physical operations of equipment. Where generation machinery such as turbines was once only mechanically operated, equipment is now mostly protected and controlled by ICS synchronously, by automation and sometimes remotely. These technological improvements have caused most power grids to be increasingly vulnerable to intrusions from cyberspace. Modernisation efforts of older grid system components to incorporate new digital automation, or smart grid technologies, have introduced a greater number of IP enabled access points to grid network [20].

The integration of IT and operational technology in ICS expands the cyber threat landscape by introducing several threat vectors as consequences of the greater connectivity of systems. Networks can become less secure over time, often being reconfigured to allow one-time access for a particular need or convenience and never being appropriately restored. Remotely accessible equipment is further vulnerable to public discovery via unprotected networks or the internet. According to Amin [21], each system of the US power grid (generation, transmission, and distribution) poses analogous and distinct vulnerabilities to the reliable delivery of electricity via cyber-physical assets.

4 Risk management framework

The proposed framework includes a conceptual view risk management areas and process to support the risk management activities. This section provides an overview of the approach.

4.1 Conceptual view

The proposed framework includes a set of modelling concepts that are essential to understand, manage, and express cybersecurity risks. We have identified a few concepts necessary for the development of the cybersecurity risk management framework that will put into consideration the cascading impact. Based on those concepts, an in-depth exploration of the numerous methods, tools, and techniques that can be used for a risk management framework in CI organisation has been performed. An overview of the concepts used for the proposed framework is explained below

Assets: assets are the tangible or intangible entities which are necessary and have values to the organisation. Identification of critical assets and putting a value on each critical asset is an important process of risk management.

Threat actor: threat actor is a group, organisation or individual operating with malicious intent. They are characterised by their location, skills, and resources used to generate a cyber-attack within the organisation as shown in Fig. 1. All the information about the threat actor should be available for risk identification and mitigation.

Vulnerabilities and threat: vulnerability is the weakness in an asset that is exploited by a threat actor. The threat is the unauthorised access to an asset as a result of a vulnerability in an asset that is been exploited by a threat actor.

Risks: Risk in the case of a CI organisation is the probable failure of an organisation to fulfil its goals such as confidentiality, integrity or availability due to the probability of a threat actor obstructing its goals.

The concepts are linked with each other through activities to support asset identification, vulnerability assessment, threat identification, risk assessment and deal with cascading effect as shown in Fig. 2. Assets are necessary for CI organisations to operate and needs to be kept secure for the continuity of the business, but these assets are prone to weaknesses in their systems known as vulnerabilities. These vulnerabilities are exploited by threat actors to attack the asset and when not addressed on time can influence a threat which introduces risk and this risk is likely to lead to the exploitation of the assets. Once the risk factors have been identified, risk assessment is carried out to mitigate them.

4.2 Process

The process comprises of a systematic collection of activities which are linked with each other to support specific tasks relating to risk management. We follow the guidelines identified in the existing risk management standards ISO 310000 [22], NIST SP800-30 framework [23], and NERC CIP standards [17] to define the process. In particular, the main focus is to understand the asset, vulnerabilities, and threats that can lead to risk for CI organisation.

4.2.1 Activity 1-assets identification and categorisation: For successful risk management, asset identification is crucial and needs to be initiated before any risk is identified. The purpose of asset identification is to identify and prioritise assets according to their criticality levels in the organisation. The resulting asset list and categorisation are then used as input to vulnerability assessment. Identification of critical assets is necessary to protect against cyber-attacks and consequential destruction. CI consists of critical assets that are absolutely necessary for its stable and reliable functioning of the organisation and cyber-attacks could have catastrophic consequences, such as loss of power or shortage of water supply. Examples include Shamoon [24], a computer virus that struck a Saudi Arabia oil company's Windows-based computers as many as 30,000, operating on the company's network. This disrupted the company's business operations, thereby causing data loss and disabled workstations. Stuxnet [24], a malicious computer worm that targeted the SCADA systems, altered and caused damages to the Iranian nuclear program. Ukraine experienced a total blackout as a result of cyber-attack on the power grid. Adversaries that successfully loaded malicious firmware into the SCADA network field gateway devices compromising its information systems and temporarily disrupting electricity supply to the end consumers [25].

This activity identifies the most critical assets of CI following a systematic approach using the asset focus. These assets are prioritised based on their impact on the organisation. This provides an understanding of what a critical asset is and how to secure it from a cyber-attack. For this activity to be efficient, it is necessary to include and engage the relevant stakeholders within the organisation, as they are the ones with insights into the system and capable of determining asset types, asset impact types, and the required level of protection necessary for each asset, including the sensitivity and value of a particular asset. The final task of this activity is attaining critical assets which is done based on the output generated from previous tasks.

Task 1A– identify assets: asset identification is the first step in any risk management process. Identifying key assets of a CI organisation and putting a value on each key asset is an important process of risk management. These key assets could be data, software, hardware, SCADA systems, and communications, and networks as shown in Fig. 3. Critical assets are defined as assets with a high consequence and high probability of failure, therefore, it is important to identify critical assets as well as estimate their critical failure modes or impact of the loss. This task identifies critical assets by looking at the following three steps:

Step 1 – Asset focus: asset focus refers to the specific assets to be considered for vulnerability and threat assessment as well as risk analysis because assets that comprise our CIs are not evenly critical. The asset focus is to be considered are software assets – program or application used by CI organisations for its business activities. If such assets are not managed properly, they may involve in compliance risks, threats to corporate reputation and even its existence. Data assets – they are information stored and used by a computer system. Hardware assets – they are the collection of physical components of a computer system, communication, and network.

Step 2 – Determine goals and key performance indicators (KPIs): this step identifies the organisational goals for the CI in terms of security and organisational context. The main goals are in general confidentiality, integrity, and availability. Based on these goals the KPIs for the organisational context are considered. It is also necessary to identify the key operational responsibilities of the CI in order to support cybersecurity activities. KPI plays an integral role in risk management. They have the benefits and targets set my organisations and these goals must be achieved. KPI is given a range between 1 and 0. Secure CI should be able to provide the below KPI conditions

- Confidentiality (*C*): this KPI deals with the disclosure of sensitive data against unauthorised users, CI internal users, external users, and malicious attackers. It involves the deletion and transfer of data between authorised users in a secure environment to prevent data leakage. One of the simplest methods to provide confidentiality is to install encryption/ decryption components at both ends of an unsecured connection [26].
- High availability (*A*): availability refers to ensuring that the assets of the CI are made available and accessible to the end users as agreed or when and where they need it. It defines the degree or extent to which the asset is readily usable along with the necessary IT and management procedures, tools, and technologies required to enable, manage, and continue to make it available. This requirement of the CI security is very important and one of the primary objective to ensure the reliable operation of the assets. Generally, availability refers to the timely and reliable access to the use of CI assets and the capacity to access the assets even under the most critical situations.
- Integrity (*I*): integrity refers to the ability of the CI organisations assets to perform its required functions effectively and efficiently without any disruption or loss of its services. It includes the critical aspect of any asset which stores, processes, and retrieves data its design, implementation, and usage. Integrity ensures that the data managed by systems and messages communicated over the network are not altered by unauthorised users.
- Reliability (*R*): this KPI allows for the CI to be able to work on an acceptable level of efficiency and consistently well even when external or internal disturbances occur.
- Authorisation (ATH): this KPI allows the organisation to specify access rights and privileges to resources related to the information of a particular actor.
- Authenticity (AUT): this KPI improves the identification and verification technology of an authorised user in order to provide security, ease of use, and administration. It has the capacity to identify an authorised user to its specific appropriate information and service type.
- Privacy (*p*): This KPI gives an organisation the ability to seclude sensitive information about themselves and their users from third parties. It involves the appropriate use, as well as the protection of information.
- Maintainability (*M*): maintainability is associated with the mean time to repair an asset and get it to work perfectly within a specified period of time. The time could be categorised as less than a day, several days, one week, several weeks, month or months and even a year.
- Conformance (CON): This KPI ensures that the assets such as services meet with the specified standard.
- Accountability (ACC): This KPI gives an assurance that an actor will be evaluated on their performance or behaviour related to something for which they are responsible.

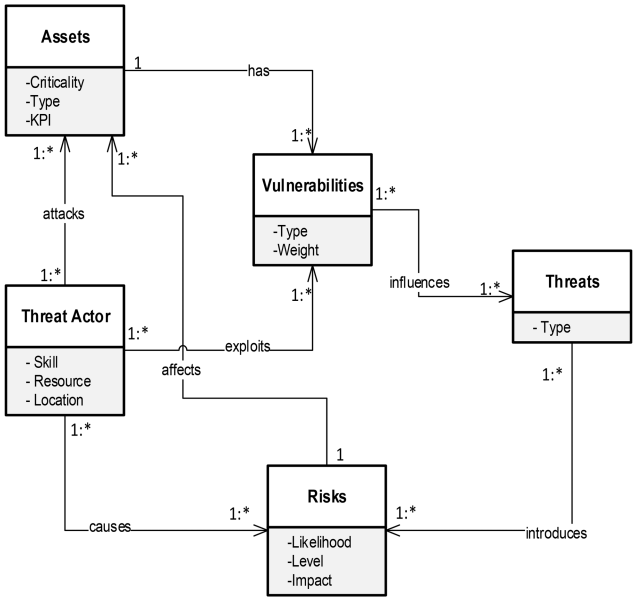

Fig. 2 *Metamodel*

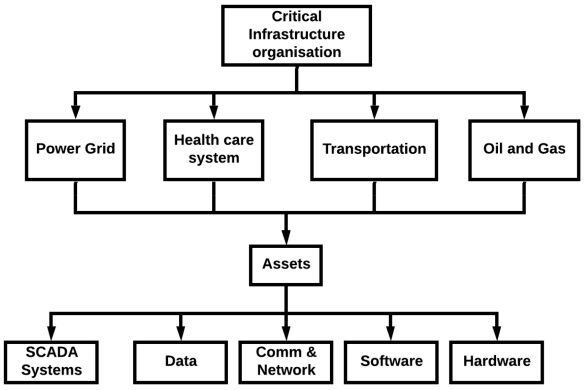

Fig. 3 *Asset categorisation*

Step 3: Identify KPI weight: this step focuses on identifying the total KPI weight for each asset. Measuring an assets KPI value requires that numerous factors are considered by using several criteria [6], such as economic impacts, financial impact, operational impact etc. The criteria represent factors against which asset criticality is measured and distinguish those assets whose loss could have a significant impact on the objectives of the CI organisation. Each asset is evaluated for all relevant categories and therefore, the number of categories is restricted in a manner to allow for feasible execution but still capture an accurate identification of the overall criticality. To get the total KPI weight for each asset, sum the total value together as shown in the equation below

$$A_{\mathrm{KPIW}} = \sum_{i=1}^{n} \mathrm{KPI}i \tag{1}$$

where A_{KPIW} = Total KPI weight value for each asset, i = 1–10, KPIi = KPI value for each asset (see Table 1 for results).

Task 1B: Determine asset criticality: criticality is the major indicator used to determine the importance of the assets to the CI organisation. This task focuses on combining the weight of an asset KPI by the total number of assets to derive the criticality level of the asset. With the growing threats and possible vulnerabilities, the need to protect our critical assets is vital, especially to ensure a well-functioning national CI. There is no standard way of combining information to determine which asset is more important than the other asset. The protection of all critical assets is almost impossible in practice due to resource limitations and budgetary constraints. Thus, with an effective identification of the most critical assets that allows ranking, it is possible to focus on those assets that, if disrupted, could have a serious impact on national security, public health and safety, and business continuity. Assets criticality is determined based on the assets total KPI weight score by the total number of assets. To separate assets based on criticality, a table considering five different categories of criticality are assigned a weighted score between zero and ten in Table 2

Equation (2) is designed to help an organisation categorise its most critical asset based on a subjective judgment by the stakeholders and other parameters used within the organisation. The total value for each assets KPI weight is summed up and divided by the total number of assets.

$$A_{\mathrm{c}} = \frac{K_{\mathrm{KPIW}}}{A_n} \tag{2}$$

where A_{c} = asset criticality, A_{KPIW} = total KPI weight value for each asset, A_n = Total no of assets.

Taking the running example presented in Section 3, the below section demonstrates how asset criticality is derived. If software's total KPI weight is 30 and the total number of software assets is 5, A_{C} is derived as

$$A_{\mathrm{c}} = \frac{30}{5} = 6.00$$

Hence, the asset critical score for the software in the example is '6.00 = medium' which means the asset is highly critical to the organisation, and that any negative impact can lead to severe damage not just to the organisation, but also to the public.

Task 1C – Asset Inventory: this task takes the results from the previous tasks and provides an asset inventory by structuring assets in terms of criticality. The asset inventory is then, in the next activity (Section 4.2.2), used as input to the vulnerability and threat assessment. The table below shows an asset inventory of the most critical assets of the CI Organisation in the running example (see Table 3 for results).

4.2.2 Activity 2 – identification of vulnerability and threat assessment: An essential part of a risk management process is to determine the vulnerability of a system or an asset and the consequence of potential threats [13]. This activity focuses on identifying vulnerabilities, causes, and consequences of threats, types of threats, cascading effects of threats, and how these might affect the system and its assets. Evaluating the level of risk posed by a system or an asset also requires an understanding of threats and vulnerabilities and the inherent uncertainties. Fig. 2 shows a conceptual overview of activity 2. In the following tasks, this activity is demonstrated using the running example where the focus is on cyber incidents targeting the critical assets of the example power grid.

Task 2A: Identify Vulnerability: this task identifies vulnerabilities on the most critical assets identified in Activity 1. Vulnerability identification could follow different techniques, but in this example, a checklist of all possible vulnerabilities associated with each critical asset is used to identify vulnerabilities. The vulnerability is an exposure to security that results in the weakness of a critical asset allowing for the compromise of any of the security objectives properties (confidentiality, integrity, and availability) [27]. It can also be defined as the measure of the susceptibility of a system to threat [13]. Identification and assessing vulnerability is an important and delicate task that has an impact on the successful operation of assets that provide CI services. This task will present a model and then apply the model to the example power Grid (running example). Identifying vulnerability is an active strategy for improving infrastructure security and provides vital information which can be used to conduct a risk analysis in the next activity. It also helps in controlling cyber-attacks and strengthens security in the weak points of a CI that leads to a serious impact on its critical asset.

There are several ways in which an attacker can exploit vulnerabilities in CI systems, and therefore causing severe damage,

from an attacker only being able to view information to a worst-case scenario. Regardless of the vulnerability discovered, the attacker could have little or complete control over the system and any action taken is referred to as a cyber-attack. The below table is a summary checklist of the possible vulnerabilities found in the critical assets of the running example. Note that the list does not represent an exhaustive list of all the vulnerabilities because it changes over time, for example, due to environmental or technical changes. In this example, the checklist of vulnerabilities from [28] is used for illustrative purposed. This checklist structures vulnerabilities into categories such as software, hardware, data, SCADA systems, communication, and network (Table 4).

To simplify the vulnerability identification it is divided into multiple steps, including evaluating various locations of an attacker, vulnerability weight based on cascading vulnerabilities effects, and evaluation of how vulnerability can affect different assets thus leading to a threat on the asset.

Step 1 – Vulnerability Impact (VI) Rating: the impact of vulnerabilities on critical assets is assigned using a vulnerability rating (VR) score of VR.1–VR.5, from very high to very low. In the case of multiple vulnerabilities, each vulnerability is assessed and given a rating score. Description of the various levels of VR is explained in Table 5.

Step 2 – Asset VI Assessment Model (A-VIAM): this step determines the VI of an asset by using A-VIAM which is built upon a mathematical multi-value theory and structured as a value model [29]. To demonstrate the A-VIAM model, it is applied to the running example. The total impact value of all the critical assets (ACs) components is summed together and divided by the total number of critical assets considered to derive the vulnerability level of the entire system as shown in (3) and (4). For example, the vulnerabilities identified for a software asset in the running example, the VR score is assigned based on its impact on the software critical asset. All the VR are then summed together to get an impact value for the Software asset and then divided by the total number of vulnerabilities identified. The same method is applied to each identified critical asset. The calculation of the A-VIAM model is shown below

$$\mathrm{VI}_{\mathrm{AC}} = \sum_{\mathrm{VR}i=1}^{n} \frac{V_{\mathrm{VR}i} + V_{\mathrm{VR}i} + \cdots + n_{\mathrm{VR}n}}{V_n} \tag{3}$$

where $\mathrm{VI}_{\mathrm{AC}} = \mathrm{VI}$ for each critical asset, V_n = total no of vulnerabilities, VR 1–5, $i = 1$–n.

Table 1 Asset KPI weighting

Asset category	Subcategory	C	A	I	CON	R	AUT	P	M	ACC	ATH	KPI weight
software assets	microsoft office	0	1	0	1	1	0	0	1	0	0	4
	mail server software	1	1	1	1	1	1	1	0	1	1	9
	master boot files	1	1	1	1	1	0	0	0	1	1	7
	windows operating systems	0	1	1	1	1	1	0	1	0	1	7
	UPS remote management interface	0	1	0	0	1	0	0	1	0	0	3
hardware assets	computer systems	0	1	0	1	1	1	0	1	1	0	6
data assets	customer files	1	1	1	0	0	0	1	0	1	1	6
	database files	1	1	1	0	1	1	1	0	1	1	8
	intellectual property	1	0	1	0	0	0	0	0	0	0	2
	personal data	1	1	1	0	0	0	1	0	0	0	4
	network information	1	0	1	0	0	1	1	1	0	0	5
	emails	1	0	1	0	1	0	0	0	1	1	5
	legitimate credentials	1	0	0	0	0	0	1	0	0	1	3
	admin passwords	1	0	0	0	0	0	1	0	0	1	3
SCADA systems	industrial control systems (ICS)	0	1	1	1	1	1	0	1	1	0	7
	HMI computers	0	1	1	0	1	1	1	1	0	1	7
	remote terminal unit (RTU)	0	1	1	1	1	0	0	0	1	1	6
	production ICS network	1	1	0	1	1	1	0	0	1	1	7
	ICS specification	1	1	0	0	1	0	0	0	0	0	3
	SCADA database software	1	1	1	0	1	1	1	1	0	1	8
	programmable logic controllers (PLC)	0	1	1	0	1	0	0	0	0	0	3
	industrial software application and windows	0	1	1	0	1	1	0	0	0	1	5
	substations Ethernet devices	0	1	0	0	1	0	0	1	0	0	3
	workstation	0	1	0	1	1	1	1	1	0	1	7
information and communication networks	company's computer network	0	1	1	0	1	1	0	1	1	1	7
	virtual private network	1	0	0	0	1	1	0	0	0	1	4
	router/modem/ switches	0	1	1	1	1	1	0	0	0	1	6
	firewalls	0	0	1	0	1	0	0	0	0	0	2
	website	0	1	1	0	1	0	0	1	0	0	4
	remote access services	1	1	0	0	0	1	0	0	1	1	5
	mail server	1	1	1	0	1	1	0	0	0	1	6

Table 2 Criticality levels

Critical level	Weight	Description
extreme	8.00-10.0	extremely critical and is of high value to the CI organisation, requires an extreme level of protection
high	6.00–7.99	high importance to the organisation and requires a high level of protection.
medium	4.00–5.99	the asset is moderately important to the organisation and requires moderate protection
low	2.00–3.99	the asset is of minimal importance and does not require many levels of protection
very low	0.01–1.99	the asset non-critical and requires a very low level of protection

Table 3 Asset identification, e.g. power grid (CI)

Asset category	Sub-category	KPI weight	(1)	(2)	Asset criticality score	Critical level
software assets	microsoft office	4	30	30/5	6.00	high
	mail server software	9				
	master boot files	7				
	windows operating systems	7				
	UPS remote management interface	3				
hardware assets	computer systems	6	6	6/1	6.00	high
data assets	customer files	6	36	36/8	4.50	medium
	database files	8				
	intellectual property	2				
	personal data	4				
	network information	5				
	emails	5				
	legitimate credentials	3				
	admin passwords	3				
SCADA systems	industrial control systems (ICS)	7	56	56/10	5.60	medium
	HMI computers	7				
	remote terminal unit (RTU)	6				
	production ICS network	7				
	ICS specification	3				
	SCADA database software	8				
	programmable logic controllers (PLC)	3				
	industrial software application and windows	5				
	substations Ethernet devices	3				
	workstation	7				
information and communication networks	company's computer network	7	34	34/7	4.86	medium
	virtual private network	4				
	router/modem/ switches	6				
	firewalls	2				
	website	4				
	remote access services	5				
	mail server	6				

Score range = 1.00–10.0 for each vulnerability associated with the critical asset; 1.0–3.99 (low), 4.00–6.99 (medium), 7.00–10.0 (high).

To demonstrate the VI assessment, assume there are three vulnerabilities (V3.1, V3.2, and V3.4) from the checklist presented in Table 6. The impact is by following (3)

$$\mathrm{VI_{AC}} = \mathrm{V3.1_4} + \mathrm{V3.2_3} + \mathrm{V3.4_4} = 11/3 = 3.67$$

In this case, the VI of the software asset is low, therefore there is little possibility of a threat occurring.

To calculate the VI of an entire system, the total VI of each critical asset $\mathrm{VI_{AC}}$ is summed together and divided by the total asset as

$$\mathrm{VI_S} = \sum_{\mathrm{VI_{ACi}}=1}^{n} \frac{\mathrm{VI_{ACi}} + \mathrm{VI_{ACi}} + \cdots + \mathrm{VI}_n}{A_n} \tag{4}$$

where $\mathrm{VI_S}$ = VI for entire system, $\mathrm{VI_{AC}}$ = VI for each critical asset, A_n = Total no of assets where i–1 to n, vulnerability range = 10–100%, where 10% (low) 100% (very high) (Table 7).

Task 2B – Identify Threats: this task identifies the possible threats affecting a CIs ability to deliver its services. CIs can be remotely controlled over the internet by the implementation of IT systems. This implementation of IT systems on CI and the interconnection between them have given room for cyber threats leading to security concerns. Threats such as the denial of service or malware attacks are famous threats to CIs causing security challenges to the interconnected devices [24]. This task also looks at the different threats that affect critical assets, therefore, creating the occurrence of a risk or risks.

4.2.3 Activity 3 – cascading vulnerabilities and risk: Accurate risk identification is essential for any critical infrastructure organisation. Our approach identifies and evaluates the critical assets, related vulnerabilities, and threat that could lead to risk. Vulnerability is defined as weakness in an asset, exploited by a threat actor who is either an individual, organisation, or a group executing a program with the intention of compromising the security objectives (KPI) of a vulnerable asset. This leads to a threat of the CI organisation and causes risk to the overall business continuity. For this reason, we have carefully considered analysing the interdependency among assets, it's likely vulnerability, a threat as a result of the exploited vulnerability and risk to the overall organisation which is known as cascading impact. This activity considers the decision tree model for risk identification due to the cascading dependency among vulnerability, threat, and assets. The first step of this activity is to determine the cascading vulnerabilities and their link with the assets. The second step focuses on the identification of the risks.

Step 1 – Identify Cascading Vulnerabilities: at this stage, it is necessary to determine the cascading vulnerabilities and their dependency on the assets. The cascading vulnerabilities occur when vulnerabilities are linked with each other to cause a threat as shown in Fig. 4. The impact of threat is higher in case of such occurrence and cause severe damage to assets and the CI organisation. Considering the running example, the power grid is attacked due to the following vulnerabilities allowing a computer worm to compromise each host and contributed to a successful attack

- Insufficient security hardening of computers rendering them unable to withstand any form of attack, therefore, leading to

- Gaining access to the network and due to lack of network segmentation, there is a successful compromise of the network causing more hosts than necessary to be attacked.
- When the network is hijacked, sensitive organisations information is susceptible for loss, theft, or damage. Inadequate response and recovery plan is not always well established to effectively restore operations and lost data. In the running example, the organisation was not able to deal with the worm outbreak at the initial response and the various stages during recovery.
- Insufficient employee security awareness training is also another vulnerability that could make an attack successful. In the running example, employees were not aware of the incidents in progress and that simple unintentional action can void the most demanding security measures.

All these vulnerabilities contribute to the opportunity and success of an undirected attack against the example CI. Fig. 5 shows cybersecurity attack scenario through one vulnerability cascades to influence other vulnerabilities which leads to a threat

Table 4 Vulnerability checklist [28]

Assets affected	Potential vulnerability
1. SCADA systems	V1.1 lack of security hardening
	V1.2 buffer overflow
	V1.3 cross-site scripting
	V1.4 cross-site injection
	V1.5 cross-site request forgery
2. communication and networks	V2.1 misconfiguration of network
	V2.2 failure to segment network
	V2.3 data path interference
	V2.4 unprotected network communications
	V2.5 open physical connections
	V2.6 single point of failure
3. software	V3.1 buffer overflow
	V3.2 weakness in authentication, authorisation, and cryptography.
	V3.3. invalidated input
	V3.4 social engineering
	V3.5 technological changes
	V3.6 design flaw
	V3.7 file sharing
	V3.8 lack of documentation
	V3.9 no log out when leaving the workstation
4. hardware	V4.1 unprotected storage
	V4.2 insecure locks
	V4.3 susceptible to dust and soil
	V4.4 hardware design flaws
	V4.5 outdated hardware change controls
	V4.6 misconfiguration of hardware
5. data	V5.1 deployment failure
	V5.2 broken databases
	V5.3 data leaks
	V5.4 stolen database backups
	V5.5 abuse of database features
	V5.6 lack of segregation
6. people	V6.1 disgruntled employee
	V6.2 lack skills
	V6.3 loss of key personnel
	V6.4 insufficient training
	V6.5 issue motivated interference
7. organisation	V7.1 lack of DR plan

Table 5 Vulnerability rating table

VR score	Criteria	Description
VR.5	very high	one or more major weaknesses have been identified that make the asset extremely susceptible to an attack. The organisation has no capability of resisting the occurrence of a threat
VR.4	high	one or more major weaknesses have been identified that make the asset highly susceptible to an attack. The organisation has the low capability of resisting the occurrence of a threat
VR.3	medium	a weakness has been identified that makes the asset moderately susceptible to an attack. The organisation has the reasonable capability of resisting the occurrence of a threat
VR.2	low	a minor weakness has been identified that slightly increases the susceptibility of the asset to an attack. The organisation has a good capability of resisting the occurrence of a threat
VR.1	very low	no weaknesses exist. The organisation has an excellent capability of resisting the occurrence of a threat

Table 6 Threat and vulnerability on CI [28]

Asset type	Vulnerability types	Threat types
hardware	lack of care at the disposal	theft of media or document
	lack of efficient configuration change control	error in use
	insufficient maintenance installation on storage media	breach of information system maintainability
software	lack of audit trail	abuse of rights
	lack of proper documentation	error in use
	widely distributed software	corruption of data
communication and network	lack of identification and authentication mechanisms	forging of rights
	unnecessary services enabled	illegal processing of data
	unprotected communication lines	eavesdropping
people	insufficient security training	error in use
	absence of personnel	breach of personnel availability

Table 7 A-vulnerability impact

Asset name	Vulnerability type	VR score	(3)	VI
SCADA system	V1.1, V1.5	3, 4	7/2 = 3.50	low
software	V3.1, V3.7, V3.9	2, 3, 4	9/3 = 3.00	low
communication and networks	V2.1	5	5/1 = 5.00	medium
hardware	V4.3, V4.4	3, 4	7/2 = 3.50	low

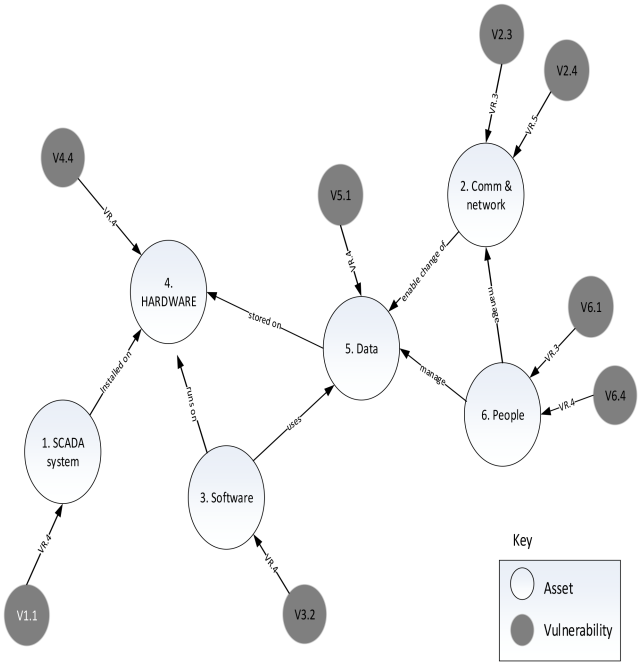

Fig. 4 *Interdependency of assets*

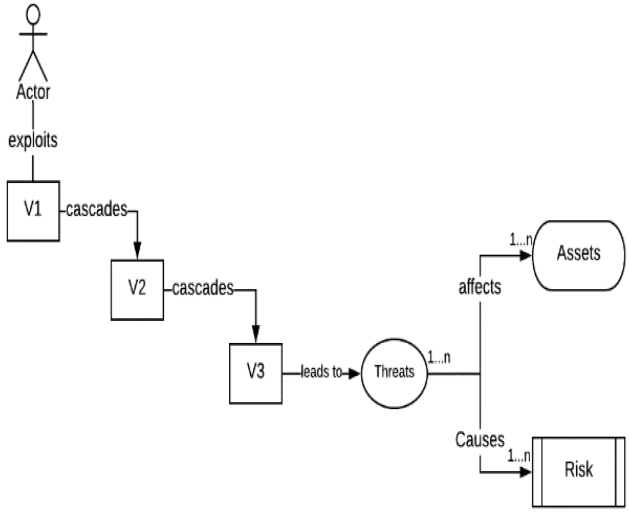

Fig. 5 *Cascading impact*

and have a negative impact on an asset or assets of a CI organisation, which finally materialises into a risk.

Step 2 – Identify Risk: this final step identifies the risk of the CI based on the cascading vulnerabilities and the threat to the assets. We follow the decision tree model to determine the risk so that appropriate control can be identified. A decision tree is a tree in which each branch node represents a choice between a number of alternatives and each leaf node represents a decision [6]. Decision trees are easily interpretable because the tree structure can be represented graphically and we can follow branches down the tree according to the input variables, requiring less processing time. It also has the ability to assign specific values to problems, decisions, and outcomes of each decision, this enables a single clear view of all possible solutions. The reason for choosing decision tree technique is that it provides a chain of events as a result of an attack and significantly improves the ability of the organisation to find new exploits in an asset and implement appropriate control measures before it escalates.

We follow the cascading vulnerability and its impact on the asset to identify the risks. In particular, the root node in our case is the vulnerability which can exploit the threat as leaf decision node as shown in Fig. 6. Vulnerability is considered as predicator for risk identification. If the threat affects the critical assets then the final decision is whether to accept the risk and undertake the necessary control. The decision tree helps in our case to consider the cascading impact which is due to an unexpected chain of events caused by the action of a threat actor which affects an asset and the organisation at large. They are extreme events in which the impact increases in progression over time and generates a series of minor events that eventually lead to a serious negative impact. Cascading impacts are often caused by unresolved vulnerabilities in a system. Cascading impacts is considered a complex problem in CI because such events result in devastating consequences to other assets or CIs [30] and as the interdependences of assets are sometimes complex. The level of the tree depends on the cascading vulnerabilities and threat which effect on the assets.

Fig. 6 shows the underlying vulnerabilities that materialise an attack; this depends on the skill and motivation of the threat actor to gain access to the system or network. The tree shows that once a threat actor gains access to any asset of the organisation, it is likely for them to carry out an attack that can lead to a major risk. This allows to predicate the high risks and helps organisation to undertake the necessary control to rectify the weaknesses in proactive manner. Decision tree demonstrates the cascading impact of vulnerabilities and threats on assets in a simple manner so that

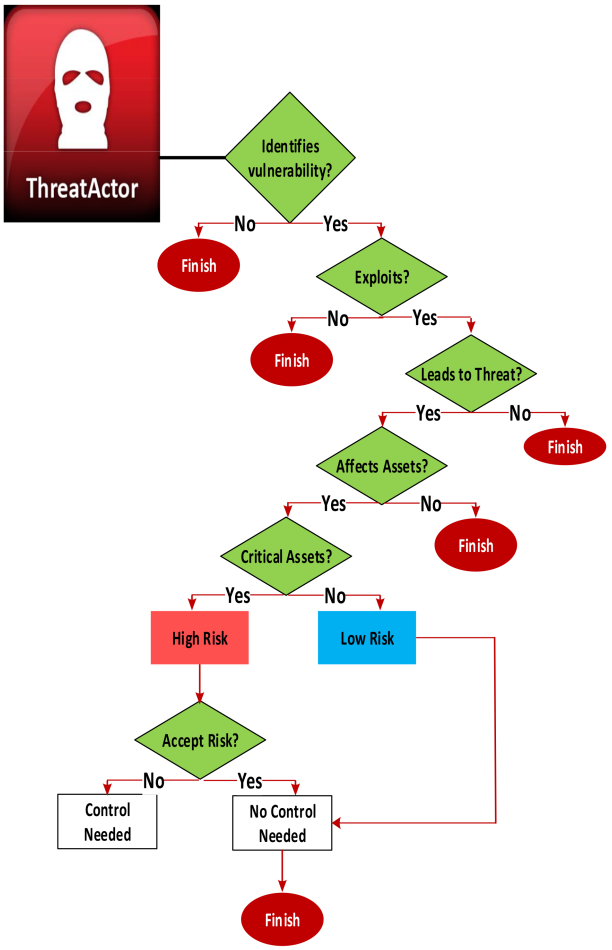

Fig. 6 *Decision tree*

CI organisation can understand which risks are important and needs early attention.

5 Conclusions

Risk management is essential for any CI organisation for protecting its assets. It is a continuous process of maintaining the effective functioning of critical assets in any circumstance. One of the critical steps of risk management is to understand the relevant vulnerabilities and threats that could pose any potential risks. This paper contributes towards this direction and focuses on three major aspects of risk management, i.e. assets identification, vulnerability, and threat assessment and risk identification. The approach follows the decision tree model to identify the risks and necessity of control based on the cascading impact of vulnerabilities and threat on the assets. This allows predicating the high risks and justifies the necessity of control in a proactive manner. The approach is demonstrated using a running example from the SCADA system of a power grid CI. The result from the running example shows that some assets are more critical than others and identifies the vulnerabilities and threats relevant to the context. The result of the study indicates that decision trees are a useful tool for modelling threats and vulnerabilities in a wide variety of systems. Future work includes expanding the focus to analysing the risk of the critical assets and to propose a comprehensive risk management process for the CI.

6 Acknowledgments

This work was financed by the petroleum trust development fund (PTDF) Nigeria. The authors thank the Commandant Nigerian Defence Academy Kaduna, Nigeria for the support.

7 References

[1] Abouzakhar, N.: 'Critical infrastructure cybersecurity: a review of recent threats and violations'. European Conf. on Information Warfare and Security, Finland, 2013
[2] Dalziell, E.P., McManus, S.T.: 'Resilience, vulnerability, and adaptive capacity: implications for system performance', 2004
[3] Harvey, J., T.I. Service: 'Introduction to managing risk', 2007, p. 12
[4] Marvell, S., Partner: 'The real and present threat of a cyber breach demands real-time risk management', 2015, p. 18
[5] Purdy, G.: 'ISO 31000: 2009 – setting a new standard for risk management', *Risk Anal.*, 2010, **30**, (6), pp. 881–886
[6] Izuakor, C., White, R.: 'Critical infrastructure asset identification: policy, methodology and gap analysis'. Critical Infrastructure Protection X: 10th IFIP WG 11.10 Int. Conf., ICCIP 2016, Arlington, VA, USA, 14–16 March 2016, Revised Selected Papers 10. 2016
[7] Bialas, A.: 'Risk management in critical infrastructure-foundation for its sustainable work', *Sustainability (Switzerland)*, 2016, **8**, (3), p. 240
[8] Fekete, A.: 'Common criteria for the assessment of critical infrastructures', *Int. J. Disaster Risk Sci.*, 2011, **2**, (1), pp. 15–24
[9] ETSI, T., 102 165-1V4. 2.1 (2006–2012)-Method and Performa for Threat. Risk, Vulnerability Analysis
[10] Clarizia, F., Colace, F., Lombardi, M., *et al.*: 'A multilevel graph approach for road accidents data interpretation'. Int. Symp. on Cyberspace Safety and Security, 2018
[11] Wang, D., Liu, C.: 'Model-based vulnerability analysis of IMS network', *JNW*, 2009, **4**, (4), pp. 254–262
[12] Ramakrishnan, C., Sekar, R.: 'Model-based vulnerability analysis of computer systems'. Proc. 2nd Int. Workshop on Verification, Model Checking and Abstract Interpretation, Pisa, Italy, 1998
[13] Ezell, B.C.: 'Infrastructure vulnerability assessment model (I-VAM)', *Risk Anal.*, 2007, **27**, (3), pp. 571–583
[14] Cherdantseva, Y., Burnap, P., Blyth, A., *et al.*: 'A review of cyber security risk assessment methods for SCADA systems', *Comput. Secur.*, 2016, **56**, pp. 1–27
[15] McQueen, M.A., Boyer, W.F., Flynn, M.A., *et al.*: 'Time-to-compromise model for cyber risk reduction estimation', in '*Quality of protection*' (Springer, Boston, MA, USA, 2006), pp. 49–64
[16] McQueen, M., Boyer, W.F., Flynn, M.A., *et al.*: 'Quantitative cyber risk reduction estimation for a SCADA control system'. INL/EXT-05-00319, Idaho National Laboratory, CSSC Report, prepared for US Department of Homeland Security, 2005
[17] NERC, C., Standards as Approved by the NERC Board of Trustees May 2006
[18] Esser, M.: 'A framework for protecting our critical infrastructure', 2017
[19] Moteff, J., Parfomak, P.: 'Critical infrastructure and key assets: definition and identification', 2004. DTIC Document
[20] Yan, Y., Qian, Y., Sharif, H., *et al.*: 'A survey on smart grid communication infrastructures: motivations, requirements and challenges', *IEEE Commun. Surv. Tutorials*, 2013, **15**, (1), pp. 5–20
[21] Amin, S.M.: 'Smart grid: overview, issues and opportunities. Advances and challenges in sensing, modeling, simulation, optimization and control', *Eur. J. Control*, 2011, **17**, (5–6), pp. 547–567
[22] Airmic, A., Irm, A.: 'Structured approach to enterprise risk management (ERM) and the requirements of ISO 31000'. The Public Risk Management Association, London, UK, 2010
[23] Cybersecurity, C.I.: 'Framework for improving critical infrastructure cybersecurity', 2014
[24] Baldoni, R.: 'Critical infrastructure protection: threats, attacks, and counter-measures'. Technical Report, 2014
[25] Liang, G., Weller, S.R., Zhao, J., *et al.*: 'The 2015 Ukraine blackout: implications for false data injection attacks', *IEEE Trans. Power Syst.*, 2017, **32**, (4), pp. 3317–3318
[26] Taylor, J.M., Sharif, H.R.: 'Security challenges and methods for protecting critical infrastructure cyber-physical systems'. 2017 Int. Conf. on Selected Topics in Mobile and Wireless Networking (MoWNeT), Avignon, France, 2017
[27] Ani, U.P.D., He, H., Tiwari, A.: 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *J. Cyber Secur. Technol.*, 2017, **1**, (1), pp. 32–74
[28] CISO, Information Risk Assessment Handbook 26 October 2015
[29] Parnell, G.S., Conley, H.W., Jackson, J.A., *et al.*: 'Foundations 2025: A value model for evaluating future air and space forces', *Manage. Sci.*, 1998, **44**, (10), pp. 1336–1350
[30] Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: 'Cascading effects of common-cause failures in critical infrastructures'. Int. Conf. on Critical Infrastructure Protection, Washington DC, USA, 2013