*sustainability*

MDPI

*Article*

# A Systematic Review of Smart City Infrastructure Threat Modelling Methodologies: A Bayesian Focused Review

**Marc Wright *, Hassan Chizari and Thiago Viana**

School of Computing and Engineering, University of Gloucestershire, Cheltenham GL50 2RH, UK
* Correspondence: mwright12@glos.ac.uk

**Abstract:** Smart city infrastructure and the related theme of critical national infrastructure have attracted growing interest in recent years in academic literature, notably how cyber-security can be effectively applied within the environment, which involves using cyber-physical systems. These operate cross-domain and have massively improved functionality and complexity, especially in threat modelling cyber-security analysis—the disparity between current cyber-security proficiency and the requirements for an effective cyber-security systems implementation. Analysing risk across the entire analysed system can be associated with many different cyber security methods for overall cyber risk analysis or identifying vulnerability for individually modelled objects. One method for performing risk analysis proposed in the literature is by applying Bayesian-based threat modelling methodologies. This paper performs a systematic literature review of Bayesian networks and unique alternative methodologies for smart city infrastructure analysis and related critical national infrastructures. A comparative analysis of the different methodological approaches, considering the many intricacies, metrics, and methods behind them, with suggestions made for future research in the field of cyber-physical threat modelling for smart city infrastructure.

**Keywords:** smart city infrastructure; critical national infrastructure; cyber-physical systems; Bayesian networks; systematic literature review; threat modelling



**Citation:** Wright, M.; Chizari, H.; Viana, T. A Systematic Review of Smart City Infrastructure Threat Modelling Methodologies: A Bayesian Focused Review. *Sustainability* **2022**, *14*, 10368. https://doi.org/10.3390/su141610368

Academic Editors: Marc A. Rosen, Martin Wynn and Robert Home

Received: 15 November 2021
Accepted: 10 August 2022
Published: 19 August 2022



## 1. Introduction

The digital revolution has led to many scientific advancements, which have increased the effectiveness and capabilities of standard technology, with one such form being smart city infrastructure (SCI). In addition, smart cities have pushed the boundaries of classical city Infrastructure, introducing cyber-physical system (CPS)s with the ability to improve overall long-term sustainability, performance, and dev elopment. Adapting both old and new systems towards technological modernization, where the introduction of CPSs can highlight a growing need in the analysis regarding attack surfaces of such devices [1]. The key issue with introducing cyber-dimensions is that it opens the entity up to a much larger attack surface, leading to vulnerabilities on cyber-aspects of CPSs leading to physical impact [2]. Cyber-security has become an important factor because these systems are highly important with many systems expansively complex in their design, leading to the need for a whole new set of threat modelling methodologies [3] using different research methods to provide a solution towards SCI CPSs.

This research analyses and critically reviews the key aspects of the different Bayesian threat modelling approaches. Bayesian networks (BN) methodologies were chosen as the focal point of the systematic literature review (SLR), where it has been shown to provide an effective fundamental process for analysing critical and smart infrastructures [4–6]. To the best of our knowledge, there are few smart city infrastructures SLRs specifically targeting the application of all Bayesian approaches for SCI. The inclusion of alternative methodologies is to look into additional techniques and methods to reinforce threat modelling approaches, which are useful to determine how best to apply the threat modelling. One

of the biggest issues regarding cyber-security analysis, especially with much larger target of evaluation (ToE)s, is incomplete information, especially when discussing cyber-attacks that have a st+ochastic nature. BNs provides a solution for this as the process can combine different sources of knowledge with the capability to break down and process incomplete datasets within the model. There are three key objectives that underpin this SLR, and form of the scope of the literature.

1. To analyse current smart city modelling and simulation literature towards understanding the key issues and challenges faced where threat modelling can be used for a solution;
2. To critically review and evaluate the current research surrounding Bayesian-based smart city infrastructure alongside unique alternative modelling and simulation methodologies to provide the best possible solution performing cyber-security analysis within the smart city environment.

The first objective is to analyse both literature and information regarding the status of SCI. Understanding the wide array of issues within the context of SCI systems and differing perspectives towards solutions can help develop and refine current proposals expanding upon their effectiveness. Hence, having these issues and challenges be a focal point for threat modelling methodologies and verifying that their application within the context of SCI is effective towards providing a pragmatic solution. Next, a critical review of the different methodologies with the primary focus on Bayesian-based approaches across both single [4] and hybrid approaches [7]. Because of this comprehensive account regarding BN threat modelling, the many different deviations should all be reviewed to see the best possible path forward for SCI threat modelling. Finally, Chockalingam et al. [8] discusses BN modelling application within cyber security, keeping other extended variants of Bayesian outside its scope. In contrast, this study will incorporate all BNs variants within the systematic literature review in order to provide coverage of all possible solutions for the problems.

The final objective is combining the information acquired by performing both previous objectives, in order to provide comparative analysis regarding the threat modelling methodologies for their effectiveness within SCI environments. Another review is Hossain et al. [9], which looks into Bayesian-based approaches towards analysing resilience in the smart grid identifying themes and context with targeted domains. This research expands upon using individually unique alternative threat modelling methodology also applied to SCI environments, reviewing the characteristics of these methodologies to overall improve the knowledge of these systems and how to go about understanding them. The reasoning behind targeting these methods towards SCI is to widen the array of different techniques, which increases the potential solutions towards being an effective methodology. Other literature reviews surrounding this topic have covered other similar scopes, which cover only typical BN threat modelling [8] or the application of cyber situational awareness for modelling [10]. To elaborate on discussions that previous reviews made with regard to the SCI challenges, issues [11], and systems [12] that comprise of the overall architecture, though these need to be considered throughout threat modelling methodologies. Furthermore, it would highlight the requirement for multiple perspectives to analyse the different metrics regarding the system of systems (SoS)s.

The alternative methodologies that are reviewed assist in developing additional knowledge, techniques, and metrics for future research. Largely different methodologies, compared to BN, which will greatly improve future methodologies, take a multi-layered and method approach. Applying Bayesian-based approaches to provide effective analysis requires enough precision for accurate inferencing [13], through tweakings of designated metric weightings. The purpose behind exploring both Bayesian and various alternative non-Bayesian approaches is to compare the advantages and disadvantages within a much wider context for threat modelling methodologies, through the reviewing of these unique perspectives of applicable techniques and metrics for understanding the SCI underlying core cyber-security aspects of resilience, interdependency, and cyber-physical. The final

objective is to provide an overview and collective synthesis of all discussed findings across all reviewed literature. They are comprised of identifying the correct best possible approach towards threat modelling vulnerability within SCI, with how this system of systems handle complex undesired events. Future avenues will be discussed in how the knowledge from this literature review can be applied to prospective SCI-based methodologies.

Other systematic reviews that have covered similar topics regarding SCI through a security lens across many distinctive disciplines, being sustainability [14], resilience and response [15], technology governance [16], and cyber-security [17]. The focus of this SLR will be threat modeling and simulation (MaS) through the primary application of Bayesian-based approaches. This article comprises seven sections. Following this introduction, Section 2 briefly outlines the research method used in the study. The following section then discusses the basic concepts that feature in the research. Section 5 details the main research findings, followed by a comparative analysis of different analytical methodologies. Section 6 offers a conclusion to the study, alongside a discussion of future research avenues within threat modelling for SCI BN threat modelling.

## 2. Systematic Review Research Methodology

An SLR was performed to identify, analyse, and interpret all the available evidence related to a specific research question, following accordance with Kitchenham and Charters [18] guidelines for planning, conducting, and reporting, as well as following a summarisation of the process structure by Wohlin et al. [19]. Klumpner and other resources were used to help structure this study's own systematic literature review protocol. This methodology protocol will be applied across the literature review process to help confine the validity and verification realms by using the system that scientifically processes the current literature. Although the source was for software engineering, the fundamentals can still be transitionally applied towards the research, with the base being the same and only the target changing. The systematic approach focuses on Bayesian methods to best understand the overall methodologies' effectiveness and applicability to the scope of smart city environmental infrastructure, and it defines and records the individual literature's collection, selection, and critical review processes. See Figure 1 for an overview of the SLR process. The web application "Eppi Reviewer Web (Beta)" was used to manage the article selection process [20]. The search string used was for the broad research area, with three main strings used to search for these articles. UK and US language variation would still return the same searches (e.g., threat modelling and threat modelling). The search strings were:

- (Challenges OR issues) AND city infrastructure;
- Threat modelling AND Bayesian networks;
- Bayesian networks AND (city infrastructure AND (critical national infrastructure/critical infrastructure) OR (smart city infrastructure).

This literature review was conducted at the start of the 27th of October, 2021, including 365 articles with 88 duplicate searches going through the systematic selection process for both "Screen on Title & Abstract" and "Screen on Full Text", which led to 65 full-text articles reviewed, of which 55 were used for analysis. The articles selected to be used within the literature review featured a wide breadth of different methodologies and individual approaches. The databases used for the SLR is IEEE Xplore, Web of Science, and University of Gloucester Discovery. Please see Table 1 for an a quick review of the amount of literature taken from the research databases.

**Table 1.** Overview of the number of articles gathered from the different databases.

| | |
|---|---|
| IEEE Xplore | 204 |
| Web of Science | 179 |
| UoG Library Discovery | 70 |
| **Total** | **453** |

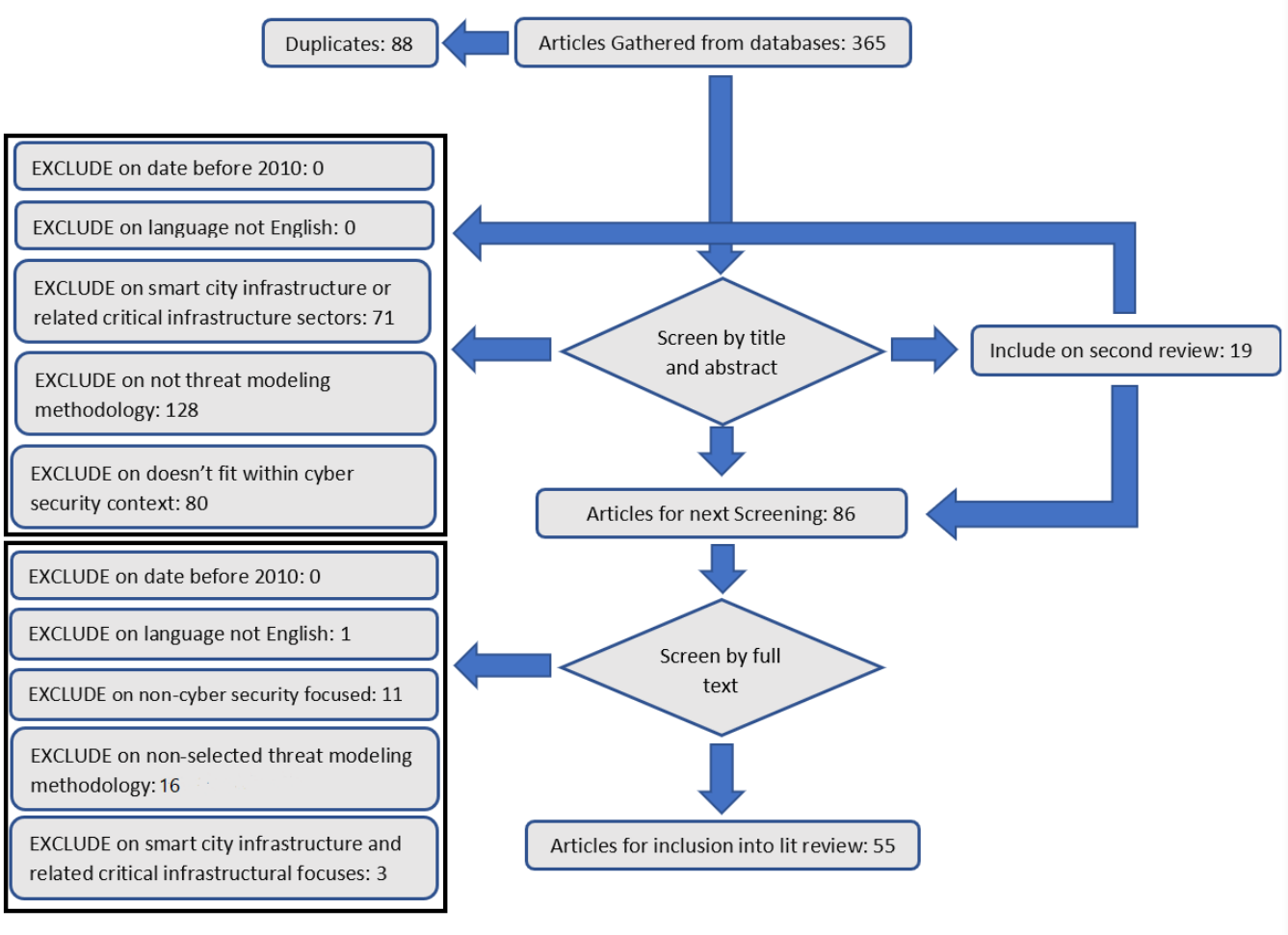


**Figure 1.** Overview of the systematic literature review process.

The UoG library discovery search engine goes through many different databases, including WorldCat, Electronic Books, Springer Link, ABI/INFORM Global, OAlster, ACM Digital Library, ScienceDirect, Business Source Complete, Wiley Online Library, PapersFirst, Directory of Open Access Journals, ProceedingsFirst, ArticleFirst, Emerald Group Publishing Limited, GPO Monthly Catalog, Electronic Collections Online, Sage Journals, Oxford Journals, Humanities International Complete, Walter de Gruyter eJournals, JSTOR Arts & Sciences V Collection, and ERIC. Consequently, the literature was broken down into four key distinct categories:

- Review of metrics, aspects, and technology implementations;
- Systematic/normal literature review of smart or critical national infrastructure;
- Bayesian network threat modelling methodology towards smart city or critical national infrastructure;
- Alternative threat modelling methodology towards smart city or critical national infrastructure.

The selection criteria are designed around the scope of cyber-security MaS for SCI, which can be accepted and declined depending on how the article fits within all Bayesian-based approaches for this specific environment by applying more general and specific exclusion criteria. Excluding cyber security is any lack of security discussion regarding both physical and cyber elements, both important to CPSs. Additionally, both threat modelling methods and SCI corresponding critical national infrastructure (CNI)s are specific to the research scope, and any articles outside of this are excluded from the review. The decision to exclude articles published before 2010 is to maintain the literature's recency and retread

old data and methodologies previously discussed or elaborated further through these models. English or translated documentation is only accepted to maintain limits within the language scope. Inclusion of the second opinion was done so when all literature was reviewed within that group, this documentation would be reprocessed. Any additional knowledge regarding the subject to make a definitive admission or rejection of the literature. Otherwise, it will be included if it does not catch any other criteria.

- Exclude on date: the study report was published after 2010.
- Exclude on language: there is no English version or translations available.
- Exclude on smart city infrastructure or related critical infrastructure sectors: the article does not fit within the project's scope regarding smart city infrastructure or any of the closely linked critical sectors that comprise it.
- Exclude on not threat modelling methodology: the paper does not discuss or propose a threat modelling methodology applied towards smart city infrastructure or related critical national infrastructures.
- Exclude on does not fit within cyber security context: the articles do not contain cyber-security focus within their analysis of smart city infrastructure or related critical national infrastructures.
- Include the second review: the paper will be coded for a second review after all other literature has been reviewed, then a decision to include or exclude shall be made.
- Include on title and abstract: include on the title and abstract, which will go through the next level of reviewing for full-text review.

The content of the articles is then processed through a more thorough lens, ensuring that all literature abides by the depth and knowledge required to provide an effective synthesis. The same criteria are reapplied through this lens, leading to fewer articles being removed at this stage of the SLR, as through the title and abstract filtering, most non-relevant articles will have been removed. However, ones removed at this level are primarily bordered or do not fit cleanly within the scope of the research review. Please see Figure 2 for an overview of the systematic literature review article mind map.

- Exclude on date: the study report was published after 2010.
- Exclude on language: there is no English version or translations available.
- Exclude on non-cyber security-focused: the article does not focus enough within the cyber-security context regarding smart city infrastructure and related critical national infrastructures.
- Exclude on non-selected threat modelling methodology: the methodology does not fit within Bayesian-based techniques or selected comparative methods.
- Exclude on smart city infrastructure and related critical infrastructural focuses: the article does not fit within the context of smart city infrastructure or other related critical infrastructure analysis.
- Include on the second review: the paper will be coded for a second review after all other literature has been reviewed, then a decision to include or exclude shall be made.
- Include on the full study: include into the full systematic literature review, where it will be used within the research articles synthesis.

### *2.1. Previous Systematic Literature Reviews*

There have been previous reviews, both normal and systematic, surrounding smart city threat modelling SCI. These reviews are Zografopoulos et al. [2], Chockalingam et al. [8], Franke and Brynielsson [10], Curt and Tacnet [21], Kalinin et al. [22], Hadjsaid et al. [23], Wang et al. [24]. These reviews highlight the need for comprehensive cyber-security planning proactive and predictive threat classification, including attack propagation and resilient architecture as a benefit for reactive counterbalances. Another key point is towards MaS of the smart city CPS. New methodologies have been researched and developed to understand the best deducing system vulnerability and implementing cyber-security analytics. One process is the usage of Bayesian networks, with an array of methodologies which can be seen

in Chockalingam et al. [8]. These are a bunch of different methods using BNs for other cyber-security analysis frameworks. Zografopoulos et al. [2] is a primary focus on cyber-physical energy systems, which is highlighted as the most important fundamental sector within SCI. It discusses the different segments that compose CNI architecture and the depth within MaS methodologies required. Another point is the emphasis on cyber situational awareness for critical infrastructure, which is the ability to compile, process, and merge data to provide a more comprehensive outcome upon a situation. Having frameworks assimilate this doctrine would assist reactive mechanisms and integrate it into Bayesian networks to provide additional structure to establish the nodes and links to improve inferencing Ahmadi-Assalemi et al. [43]. The uniqueness regarding this SLR in comparison to previous reviews is the incorporation of all BN variants, adopting both dynamic [25] and hybrid approaches for threat modelling SCI.

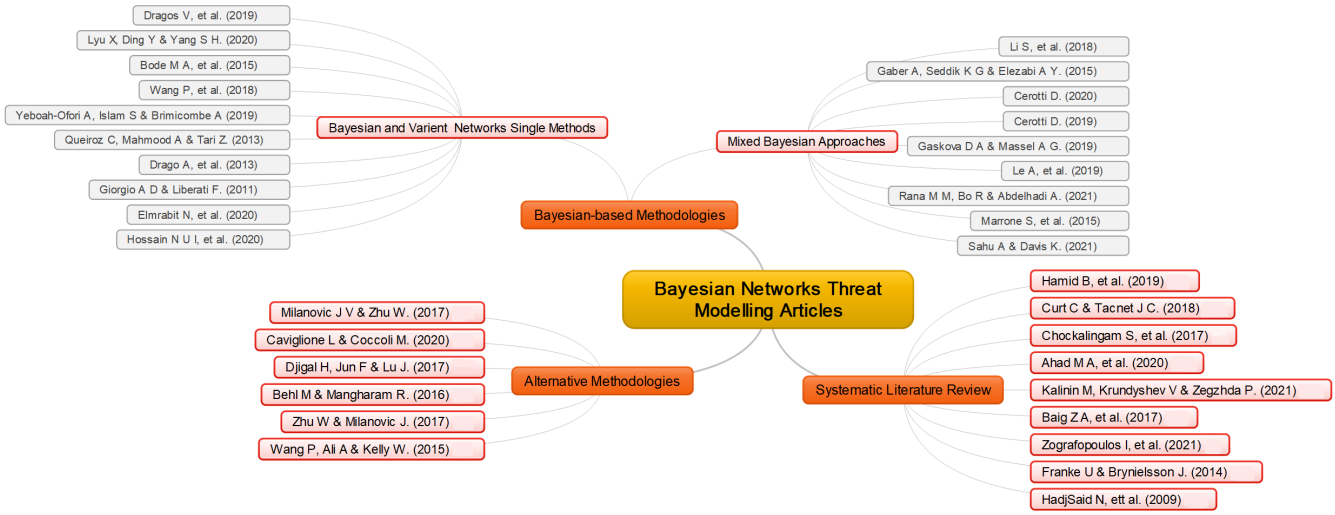


**Figure 2.** Overview of the different chosen literature within the systematic review [2,4,6,8–11,13,14,17,21–42].

### *2.2. Review Limitations*

There were some limitations present within the SLR. First, because of the main focus on BNs, there is a weakness for having included a few unique methodologies, which by default limit the process of finding the most effective framework. Furthermore, expanding the data gathering with a much scope of research databases would likely expand upon the chosen literature pool. However, these limitations are negligible as the scope for this review is around the effectiveness of Bayesian application within SCI, which for this specific purpose is suitable for the current project.

## 3. Background and Concepts

### *3.1. Critical National Infrastructure*

CNI makes up the backbone of a nation. The UK Joint Committee, which reviews their national cyber-strategy, discusses their currently designated critical sectors: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water [44]. These point out that the government must now consider the interdependence complexities. Additionally, each nation has different designations and justifications for their CNIs, leading to them having identified other sectors and sub-sectors within their frameworks [45]. However, they all share similarities across the sectors and sub-sectors, meaning that analysis can be applied across different national-framework structures. These systems are comprised of CPSs, which operate across both physical and cyber domains. These systems have additional capabilities through introduction industrial internet of things (IIoT), giving net capabilities the ability to monitor and

control. One of the core principles when conducting cyber-security within CNI architecture is its capable resilience against adverse events. The systems must handle negative events through either system failure or negative events, as the loss of these systems causes a major threat to human life and other long-lasting impacts if disabled.

### *3.2. Smart City Infrastructure*

Smart cities encompass critical systems in city infrastructure being implemented with improvements to interactivity, networking, and monitoring technologies across all aspects of daily life. Some of the technologies, such as internet of things (IoT), allow for integrating networking capabilities across a wide array of devices, with the adoption of sensors to help facilitate data collection for a multitude of purposes. Many governments are beginning to pursue the adoption of SCI. For example, the UK discusses the advantages offered and current progression into smart cities [46]. New and previous aspects will develop telecommunication capabilities, allowing for the transfer of data and individual interactivity between these systems. Cyber-security aspects of SCI, within the much wider field of CNI and critical infrastrucure interdependency (CII) research, are developing the best possible solutions through analytical frameworks through identified metrics to counteract malicious activities. Smart grids are a current development within these systems where their core goal is the inclusion of both utility and customer system interactions. Improvements across a wide array of different areas regarding environmental, reliability, and energy capabilities [47]. However, these enhancements to energy sectors highlight new attack surfaces that further complicate cyber-security implementations and magnify the intensity of preceding vulnerability.

### *3.3. Critical Infrastructure Interdependency*

A core aspect of both smart city systems and critical national infrastructure is their inherited interdependence, split across four different dominions physical, cyber, geographical, and logical [48,49]. Being both complex and intertwined, this system of systems can lead to the major issue of cascading failures, where the failure can lead to a rippling effect throughout the national level. First, individual failure can cause other entities to lose functionality and influence, while others, such as cyber-attacks, affect a certain device to control the overall system's effectiveness. Secondly, the failure of specific SCI or CNI leads to the failure or impacted effectiveness of other CNI sectors within a larger context, causing cascading failure down these relationship webs. Understanding the relationships between the different sectors and sub-sectors is necessary to understand how individual and sector-wide impacts identify the key contributing influences. The application of weighted metrics towards these influences can help provide a comparative perspective across them, allowing a much further in-depth analysis regarding identified CII [50], where threat actors can exploit these newly developed systems and cause these cascading effects throughout their targeted system and affect other key critical infrastructures.

### *3.4. Threat Modelling Cyber-Physical Systems*

Cyber-security analysis is an important component in developing truly effective defensive mechanisms. There are an array of different threats that target SCI critical sectors, which can be highlighted in cyber-attacks targeting the smart grid. Many traditional threat actors can affect these systems similarly to typical computer systems. However, the impacts that they can make through technologies, such as CPSs, has much higher importance and cause for concern [26]. Modelling both the SCI and its interdependencies is one of the newer research areas, and most proposed methodologies provide a theoretical framework for understanding these complex systems and how threats can propagate and influence the entire ToE. Many different directions of threat modelling can achieve across systems to identify the objects determining their corresponding risk and vulnerabilities, which is used to provide informed decision-making on how best to implement cyber-security. CPS has caused previous typical models to be ineffective against these new systems [51],

which has led to the further development of them or the creation of new methodologies through different technologies able to test for casual relationships and multi-layered system architectures. Similar to risk assessment methodologies, the objective depends on the methodology reviewed, where risk regarded to the system is calculated through values associated with resilience and other associated metrics. For example, vulnerability analysis focused methods look toward the success of a malicious cyber-attack against the modelled node. In contrast, risk-based approaches highlight the threat actors' actions that could affect the system through variables of probability, damage, and likelihood [27]. Both focuses are key to understanding the complex nature regarding SCI, which attributes can be heavily dissected to understand ToEd systems fully.

### *3.5. Bayesian Networks*

BN is a probabilistic graphical modelling methodology which is a directed acyclic graph (DAG) [25] that has an array of purposes. First, it can be used to model the complexities of CPSs and has been at the forefront of proposed research methodologies [8]. Second, Bayesian models use nodes representing their conditional probability table (CPT) and their individual directed links between them, which can be used to calculate uncertainty. Third, CPTs are generated through interfacing from either expert opinion or data-based approaches [13]. Finally, these models can be structured through an array of different node types, dynamic complexities, and interactions between each other [52]. These benefits highlight Bayesian approaches as an effective method to understanding the complex intricacies regarding SCI, with the capabilities to MaS the interdependencies [25] regarding CPSs and understanding the relationships between both individual systems and sub-sectors to predict the cascading effects throughout the overall infrastructure.

There are many different alternate variations of BNs, such as dynamic Bayesian networks (DBN)s, which incorporate the concept of time, taking the form of temporal nodes within the model. This methodology can be more extensive in breaking down the targeted system into discrete or continuous temporal variables tracking changes throughout a time series analysis [22]. Its main purpose is to provide probability calculations regarding individual entities and events for distinguishing the probability of effects, such as cyber-attack propagation, impact, and cascading failures [2]. These characteristics highlight Bayesian-based approaches' potential for providing a pragmatic solution. Developing and synthesising BN threat modelling methodologies have tailored individual characteristics that direct the conclusion provided through the analysis.

## 4. Systematic Literature Review

### *4.1. Issues and Challenges within Smart City Infrastructure*

The biggest takeaway from identified issues and challenges within SCI is the complex characteristics of implemented modern technologies. Typical threat modelling methodologies are currently unsuitable for cyber-physical systems because of their focus on primarily cyber-elements within their analytical frameworks where physical and CPS elements are required to provide a solid understanding of these systems. The new research area surrounds SCI and CNI to provide theoretical to verifiable frameworks, models, and methodologies. These issues can be highlighted in Baig et al. [28] through discussion on the wide array of entities present within the SCI, especially introducing CPSs allows for both domains to interact directly with one another and the interconnective processes. Although improvements to performance and communication are clear, this has increased the risk of these devices attacking where malicious actors can now interact and cause further devastation. Furthermore, these devices can output the overloaded amount of data within this landscape. Another article by St. John-Green and Watson [53] discusses the characteristics that smart and critical infrastructure challenges contend with when cyber-security countermeasures are proposed. The three major attributes of hyper-connectivity, complexity, and unbounded design of current systems alongside excessively rapid technological capabilities have led to cyber-security methods, techniques, and tools becoming further behind the

already catch-up game. They discussed the challenges facing smart and critical infrastructure cyber-security and the many aspects that researchers must review and design new methods to understand best the new environment, structures, and ramifications of an interconnected world.

An overview of the issues and threats facing them can be seen in Hamid et al. [11], which discusses the components within the city where smart technologies will influence the most: governance, people, economy, living, mobility, and environment. However, it provides an incomplete picture as the smart grid is also an influential sector, with everything coming online and requiring computational capabilities alongside itself, becoming networked across all systems. Caviglione and Coccoli [29] puts forward an analysis of the different threats and holistic model to identify and classify threats/vulnerability characteristics towards an e-learning framework within the smart city environment. Although the model is simple enough, the discussion it shows heavily indicates that the different smart layers and paradigms that methodologies must contend with if they are actually to protect against such threats. The best way is to use a concoction across the different data spaces within the sector and perceive the related constructs within the addressed architecture. Discussions into modelling CNI are heavily linked with SCI because it represents a collection of sub-categories. Therefore, analysis of threat models and simulations that look into these characteristics are also an important step in best understanding the situation. New methodologies to assist in the security of SCI must be developed [22] and should also include viewpoints from CNI security perspectives. One such current method is the application of Bayesian networks towards analysing, predicting, and simulating CPSs within the SCI and CNI.

### *4.2. Smart City Threat Modelling Methodologies*

This systematic review differs in its approach by focusing primarily on the different Bayesian methods towards SCI. The wide range of proposed BN methodologies targets similar issues within the smart city environment, with variance in their techniques and processes on identifying, analysing, and perspectives on the attributes of the systems. The inclusion of some non-Bayesian methodologies has also been looked into for further identifying viable metrics, processes, and features within smart city architectural systems and linked CNI, where a merger of these approaches could be performed within the BN framework or layered approaches.

#### 4.2.1. Bayesian Network Methodologies

Traditional threat models are too restrictive and do not adequately capture the complexity within CPSs, leading to an ineffective or missing analysis impacting crucial cyber-security aspects [54]. BN approaches are a step towards improving upon traditional cyber-security methodologies by identifying adversary capabilities, protentional failures, and system features. The primary area that these methods touch upon is related to SCI, CNI, and industrial control system (ICS), with these areas sharing an overlapping set of important sectors and features for a functional smart city. Drago et al. [27] proposes a model-driven distributed vulnerability methodology to provide the best complex cyber-physical system, using the graph-based model to identify and expand metrics to highlight attack probability and cascading features. One of the issues is the lack of cyber domain analysis in the context of CPSs, which does not provide a holistic picture in regards to the railway networks sub-sector security.Queiroz et al. [4] is a Bayesian network approach understanding system of survivable probability for SCADA-based systems, expanding upon previous methodologies through analysing services and their interdependencies within the system. One of the limitations presented and attempted to solve this is because of the interconnected nature and many influences affecting an individual node, which can cause CPTs to expand considerably. The issue occurs with other methodologies that use BNs and variations. Other BNs also applied multi-levelled application techniques across two different levels. Wang et al. [30] is a two-level Bayesian network used to identify

cyber-attacks at the general-level variations, then to distinguish them into their more specific classification. Although the methodology logic makes sense with Bayesian networks assistance for improving cyber-security using attack indicators, a key issue is lacklustre training and experiment demonstration. KDD99 is an old dataset used to train intrusion detection. With the environment of smart city infrastructure being complex across cyber and physical domains, it would lead to an ineffective security application.

Elmrabit et al. [31] proactively uses Bayesian networks for insider risk prediction analysis based on both technical and non-technical indicators through the usage of questionnaires towards identifying insider cyber threats. Although this paper does not primarily focus on insider threats within the smart-sector environment, the characteristics discussed and complex processes should be adapted to prove a tangible solution. BNs are an effective method for handling human interactions [8], through modelling the aspect characteristics and psychological aspects. Le et al. [6] is a smart grid framework using a combination of factor analysis of both factor analysis of information risk loss event frequency (FAIR LEF) and Bayesian networks to identify cyber-attacks, applying these cyber threats within the "Improving the Robustness of Urban Electricity Networks" (IRENE). The methodology does provide a structured process for analysing these attacks. However, there is a lack of discussion regarding the physical components of current or protentional cyber affecting physical attacks.

Yeboah-Ofori et al. [32] proposed a BN methodology for identification and analysing cyber supply chain (CSC) attacks within CPS using malware propagation through the ToEd system regarding cyber-crime. The malware is then broken down into six distinct categories. The methodology does not consider the CII aspects within the attack supply chain evaluation, both incoming and outgoing influential relationships. Another methodology is Hossain et al. [9], a modelling resilience framework using Bayesian networks within the systems of systems architecture for predictive vulnerability analysis, validated through sensitivity analysis to identify the most influential node. An array of many different metrics show the wide variety of technologies that the smart grid contends with or shares relationships with one another. One method to improve refinement of the methodology is applying it to live systems, which would help expand the identified metrics and their relationships. Alternatively, Bode et al. [33] is a cyber-situational awareness risk analysis using Bayesian networks, using risk matrices towards providing a software solution. One of the big issues when considering this for cyber-physical comparison is the usage of KDD cup 99, which, although a popular option, would lack effectiveness against SCI and CNI because the threats it is trained against are not affecting all aspects of the ToE. Analysing these methodologies shows the application of BN for casual modelling across SCI, especially the local CII.

#### 4.2.2. Adjusting Typical Threat Modelling Methods

Some literature has adapted current cyber-security frameworks toward the new technology architectures. For example, Cerotti et al. [34] by proposing Bayesian networks and attack graphs for analyses and detection of cyber-attacks towards smart grids, utilising MITRE ATT&CK event classifications as the backbone of the framework, using current standardised threat modelling methodologies with more complex predictive and diagnostic methods. These could bridge the current issues with the new technology and can also be seen in other research, such as adopting STRIDE [51]. Although SCI systems discussed have many intricacies, using old proven methodologies would be a good starting point as the cyber-aspects they envelop are still present with smart strategies. However, as previously mentioned, there is a gap within the current methodologies where they are incompatible with CPSs, henceforth are limited in their actual analytical security effectiveness.

#### 4.2.3. Dynamic Bayesian Networks

Some research points to the application of DBNs to adequately model and simulation Bayesian approaches, with the time aspect being a key component for more understanding of SCI. For example, Cerotti et al. [35] applies a dynamic Bayesian approach toward pre-

dictive and diagnostic analysis of distributed energy resources, also using similar attack graph processes to bolster the designed network. Di Giorgio and Liberati [25] proposes an interdependency modelling analysis framework for critical infrastructures through the application of DBN, spread across three different identified layers; atomic events, propagation, and services. DBN-based approaches appear to be a more effective methodology towards SCI, especially with their incorporation of time to properly model threat resilience. Throughout constant/discrete time-slices to examine if the ToE is authentically accurate. Through this, DBNs excel at monitoring and predictive tasks of adversarial attacks, which can be especially useful in determining through tracking the affected aspects of severe attacks via inference tasks.

#### 4.2.4. Mixed Bayesian Methodologies

Some research methodologies have used Bayesian approaches alongside other methods to help further understanding and add another process to which selected metrics can be analysed. These adopt a wide variety of alternative approaches. One of these is Gaber et al. [55] threat modelling methodology for joint-estimation detection of cyber-attacks within the smart grid, using both Bayesian and Neyman–Pearson optimum test methods, expanding upon a previous research methodology by Tajer et al. [42], with the advantages of checking the decision rules regarding the BN model providing absolute values. Another proposal is Gaskova and Massel [36] which applies dynamic cognitive maps alongside Bayesian networks for analysing cyber-threats to understand the relationships across the identified weights in respective time-scales. Expanding upon this by including DBN application after designing the cognitive maps could help maintain the flow of time throughout the system modelling and a more powerful metric transition. Rana et al. [56] is a distributed grid state-estimation framework for systems under cyber-attack by applying optimal filter theory, identifying corrupted or impacted data by cyber-attacks through local and consensus gains. However, the lack of CII can weaken the impact this methodology can have within SCI smart grid analysis, with both the interdependency both within the system and outside influences.

Other mixed methodologies include Drago et al. [37] usage of entropy metrics with the uncertainty representation and reasoning evaluation framework (URREF) ontology alongside Bayesian networks for understanding cyber-threats detection, and Marrone et al. [38] looks into applying two unified modelling languages to both the cyber SECAM plus generalised stochastic Petri nets and a physical CIP VIM plus BNs applied approach and synergised between both the profiles to threat modelling railway system infrastructure. Finally, Lyu et al. [26] uses a hierarchical Bayesian network to analyse the risk of cyber-physical systems, proposing its method of cyber-to-physical (C2P) risk assessment. The significance of cyber's impact on the physical domain can be highlighted in previously mentioned cyber-attacks. This kind of reasoning across the multi-layered approach can look into the interconnected layers and understand CPS-based architecture relationships.

Some of the reviewed methods apply intertwined Bayesian approaches, having a unique implementation to the usual. For example, Liu et al. [7] qualitative cyber security methodology towards ICS using CPSs designed attack paths, then calculating their weights through modelling attack propagation between nodes through a mixed-strategy incomplete Bayesian attack–defence approach to solve the refined Bayesian Nash Equilibrium. Alternatively, Li et al. [39] puts forward a dynamic security evaluation framework using hybrid Bayesian risk graph (HBRG)s interconnected with hidden Markov model (HMM) for a two-layered model to identify user activity patterns with a social media context. The methodology could be substituted from human analysis towards the CPS-focus, which allows for a better understanding of a mixed objective approach towards both and influences the relationship between identified nodes. Finally, Sahu and Davis [57] application of Bayesian attack graphs using structured learning techniques towards understanding cyber-physical architecture using score-based learning, expanding its scope to incorporate CPS interdependency and layered modelling across associated attributes would help

demonstrate a complete picture regarding ToE SCI. Reviewing the many different reviewed methodologies highlights a critical advancement avenue from which the SCI threat modelling can pursue. BN suitability for CPS modelling following an additional alternative method provides a fundamental backbone within proposed methodologies.

#### 4.2.5. Proposed Non-Bayesian Methodological Comparison

Although the primary focus is to review various Bayesian-based smart city infrastructure methodologies, analysing and understanding the variety of other alternative methods surrounding SCI help to broaden perspective with different used metrics that could be applied within BNs approaches. Caviglione and Coccoli [29] provides a holistic cyber-security e-learning for SCI using three homogeneous spaces for consideration of all attributes to classify threats in both a standardised grouping and its most specialised variant. Alternatively, Djigal et al. [17] secure framework for developing smart city infrastructure called "SEFSCITY" to provide governance towards an array of technologies and characteristics within these systems. These approaches offer different perspectives from previous Bayesian-based methodologies and use more mature methods within the cyber-security sphere.

Zografopoulos et al. [2] put a typical analytical cyber-physical energy sector framework towards adversary and attack model threat methodology forwards and demonstrates the security landscape of the energy sector. In addition, these entities identify attack motives and capabilities of cyber-attacks. A different approach by Wang et al. [24] provides towards smart city cyber-security with a technical and business perspective based around metrics across various areas from their literature review, which is a general framework that lacks any account for primary cyber-physical systems regarding SCI architecture. Behl and Mangharam [40] use a data-driven regression tree model to construct designs and query-response systems of identified smart city infrastructure's key metrics to provide recommendations for SCI. The model does cover the interdependency between reviewed metrics associated with vulnerability and restorative of targeted systems. However, it lacks the expansion of DBNs with time and a thorough analysis of how threats interact with the node states throughout the model. Finally, Zhu and Milanovic [41] proposes modelling of cyber-physical systems infrastructure and interdependencies by applying three-dimension weighted complex network theory to assist in identifying and analysing vulnerabilities and further cascading failures with additional usage of graph theory. Across the reviewed alternatives, one key point they could be brought further by being used alongside BN approaches as a secondary method.

## 5. Findings: Comparative Analysis of Different Methodologies

The sections correspond to each objective flows throughout the overall document, mixing in discussion regarding the literature review and the comparative findings regarding the collective methodologies. Each aspect of the SLR complies with the scope of the research project and accomplishes the set-out goals throughout its progress, as can be seen in the findings section.

1. To analyse current smart city modelling and simulation literature towards understanding the key issues and challenges faced where threat modelling can be used for a solution.
2. To critically review and evaluate the current research surrounding smart city infrastructure Bayesian-based alongside unique alternative modelling and simulation methodologies to provide the best possible solution performing cyber-security analysis within the smart city environment.

### *5.1. Objective One Findings*

Previous literature discusses both the topics surrounding issues and challenges and other SLR to synthesise the current research. The issue and challenges focused are in regards to the technical cyber-security aspects of smart infrastructures, looking into the layered architecture for CPSs. Here are some of the key issues that threat modelling

methodologies must consider within SCI environment provided, in connection with the discussed literature from the SLR.

- Security focus towards CPSs as integration increases attack surface: SCI is constructed with the introduction of Industry 4.0 technologies, which constitute the introduction of CPSs and with the issues that come with having all devices be able to network.
- Understanding of the complex interconnected nature regarding SCI: this is further complicated from the previous issues regarding cyber-physical elements, which can make the system excessively complex with the objective relationships local, national, and global levels across different interdependency layers.
- Identification of associated CPS system metrics within the smart city context: many different systems have an array of both internal and external components that affect how interlinked systems are effective, which furthermore are varied in their influences and valuations.

Other issues mentioned by both literature and literature reviews fall within one of these categories and is more specific issues regarding additional research or differing perspective outside this research scope. These are issues that attain privacy and social and political aspects. Modelling is a solution to most of these problems regarding SCI, which BNs can provide an appropriate solution for exploring this type of architecture in considerable depth, with theoretical simulations for SCI and related CNIs, with a heavy emphasis regarding MaS of smart grid systems where all three major issues are regarded. Bayesian-based modelling is effective in modelling much larger and interconnected relationships with the wide array of identified and selectable metrics valued to understand the ToE systems.

### *5.2. Objective Two Findings*

The literature reviews follow the systematic processes to identify where further research could be taken and what current methodologies are preserved to be the closest state of the art. Other SLR for cyber-security Bayesian-based modelling discusses different environments, but the main weakness is its only focus on typical BN applications. It was able to discover a gap within the research to take it further by both specialising it towards SCI and incorporating additional Bayesian variants, both dynamic and mixed. In comparison, alternative methodologies were reviewed alongside the focus on Bayesian to compare its application, metrics and influences to form a much more impactful comparison to justify Bayesian threat modelling. Further research goals to develop new or improve current processes through the valued application of metrics and influences. Discussed in the SLR and collective for the methodology's comparative analysis.

#### 5.2.1. Modelling Process and Structure

This section analyses different Bayesian and alternative methodologies based on seven characteristics, demonstrating the differences and similarities across the approaches, but where they all still share the same core objective regarding SCI or applicability towards associated smart CPSs. The main points regarding reviewed methodologies are the primary and secondary methodologies, alongside their applied metrics towards their ToE leading to their unique applications of Bayesian approaches. For example, refs. [4,9] both target understanding CNI resilience against threats, with core differences in approaches being BNs and DBNs. Most prominent are the secondary methods across BN methodologies, such as attack graph, Neyman-Pearson forms (NPF), and HMM. attack graphs (AT) shares a similar design process to BNs, where it was used previously to help develop their structured design, leading to easy adaptation into Bayesian complexity. See Table 1.

Bayesian-based approaches are scattered across BN, DBN, and hybrid variants, used to compare casual representation models under uncertainty effectively. The conjecture regarding expert knowledge to provide predictive measurements through expert knowledge is flexible in their approach. However, it is also highly subjective regarding weights associated with different key metrics across the ToE within the context regarding SCI. To compensate for this, most of the methodologies adopted a duel-modelling method approach through

supporting logic [37,56] or supplementary methods [6,38,55] to further improve the accuracy and reliability of proposals. Furthermore, they provide an effective representative conditional overview through node CPT for specifically insider threats, which can be seen in [31] BN work and could be studied into how it could be applied for a CPS. However, not specific within SCI, it could be adopted and leads to the need for further research into modelling CPSs insider threat analysis. However, one of the main characteristics that must be analyzed is the resilience of CPS systems facing uncertain/random adverse occurrences, which are most systems in SCI. For a completionism approach towards system analysis, DBN approaches [25,35] should be adopted as they include discrete/continuous time slice attributes and processing within the modelling, as resilience testing must consist of temporal factors to provide an impactful understanding. Previously reviewed normal BN approaches could be evolved into dynamic forms, where restructuring to include temporal nodes would greatly improve upon their protentional analytical capabilities. Alternative methodologies are reviewed, comprised of individual solutions, which provide their perspectives and understanding of various systems regarding SCI. They break down systems different from BN approaches and are structured much more different, such as Zografopoulos et al. [2], Zhou et al. [5], Caviglione and Coccoli [29], which demonstrate smart grids and other critical infrastructures different towards similar goals. These alternative options can be applied alongside a Bayesian-based approach to creating a new structured methodology to assist in understanding these systems and compensate and improve all aspects regarding the ToE [36]. Cyber threats are used corresponding within the model to test cyber-attacks on how the proposed framework could best understand the systems and walk through these attacks on how they influence the modelled nodes and values. These can be tested through a network by propagating cyber-attacks to predict interactions, impacts, and defensive mechanisms to counter specific or future malicious events.

However, there are weaknesses present within Bayesian-based unidirectional simulation approaches that can weaken the effectiveness regarding threat modelling, and more specifically, the SCI environment. More specifically, BNs have limitations regarding the size of the network and individual joint distributions as much larger networks can become overly complicated, especially when modelling the web of relationships between CPSs. Otherwise, most proposed solutions are still contained within a theoretical framework, which means that the systems prior probability distributions are to be played out and designed. Doing this requires a large amount of information and knowledge regarding the targeted system, where corrections and adjustments to values will need some degree of live testing to acquire accurate values. Developing these to the best possible attempt is an extremely difficult task without being applied within an entire system, designed by individuals/groups of experts or machine learning. Additionally, the further complexity upon layering the different aspects regarding the ToE, can cause largely excessive complex BNs, where the CPTs relationship links become too intertwined and become too large for computational processing power or easier understanding of the system depending on selected metrics. In contrast to the alternative methodologies discussed, which either share or avoid having these weaknesses, a mixed approach could effectively evaluate these issues within a proposed framework. However, this would require additional analysis depending on the combination used towards the specific smart city environment.

#### 5.2.2. Modelling Metrics

Metrics identified and applied throughout the different methodologies are regarding the specific categorisation within the cyber-security context. These metrics are identified across a wide range associated within the three domains regarding cyber, physical, and cyber-physical layers. An important component regarding MaS as it comprises the nodes and states defined within the methodology scope. Different metrics associated with different dimensions of threat modelling for SCI. The methodologies' purpose and overarching scope dictate which category of these metrics they will primarily focus on, but there will

still overlap, especially regarding CPSs being a core component of smart cities. Please see Table 2 for an overview of categorised metrics.

- Reactive Restoration—resilience, recovery, and redundancy of associated CPS, which is important because of the nature regarding CNI for them to either return to full functionality and mitigate adverse events to maintain functionality.
- Physical Proactive Countermeasures—physical evaluation and monitoring of physical-domain of systems. These are physical elements and processes usually seen with typical CNI systems.
- Cyber Proactive Countermeasures—analysis and review of the network, local and external-based devices, where it can be seen within supervisory control and data acquisition (SCADA) or transformed previous physical-only systems [58].
- Threat Characteristics—dictate the different characteristics regarding that specific type of cyber threat, which can be used to provide a taxonomy of identified threats.

A key component of analysing methodological metrics is assigning weighted values, accordingly, analysing throughout the entire ToE system best to identify characteristics, such as individual or overall resilience. Most of the metrics throughout the reviewed articles are associated with the cyber-domain towards all attributes considered when implementing analytical methodologies. Because cyber is the most important component within CPS systems, networking and managing these also increases the attack surface, which threats can exploit. Analysis across the physical, cyber, and cyber-physical layers requires certain metrics to provide a cross-layered approach to better understand all metrics. Specific metric interdependencies can be highlighted within BN through this, identifying what links each node within either direction as an effective method of identifying casual model relationships. Specific interdependency Bayesian-approaches [9,25,26] with how the nodes influence throughout the model. Metrics heavily side towards cyber as this is the most influential aspect regarding CPSs, especially within SCI as it underpins the networking functionality and is the main route to causing negative events, and because of this is where mostly all MaS will focus on with some focusing on human-factors which still impact these systems [31].

#### 5.2.3. Testing Methodologies and Validation Methods

The main test methods used throughout the different research articles can be classified as case study, simulation, or experiment with some variation in their approaches toward demonstrating their methodology. These stay within a confined theoretical basis for demonstrating the process throughout the ToE allowing for development and tweaking throughout, allowing for specific adversary events through the system to be analysed and identification of metrics are influenced supported by example case studies. However, the issue with this approach is the rigidness regarding MaSed events cannot fully capture interactions within the system. Further progress made within current and future threat modelling methodologies would be implemented into real-life systems. Overall, they are improving by providing live system data, which improves all aspects of the system, including bespoke reactions of the individual stakeholders regarding impacted adverse events and highlighting higher-level metrics. Another support validation method used is expert opinions applied to six reviewed methodologies. The method is applied to provide additional perspectives toward the valuations regarding the associated metrics with each processed framework and is a core component regarding the nature of BN CPTs. An issue with this is that it has a very subjective nature where its assigned weightings could be unrealistically ruining the entire MaS [32]. Please see Table 3 an overview of the different metrics associated with the reviewed methodologies.

**Table 2.** A collection of the different metrics that are used by the reviewed literature, collected to show an array associated across them.

| Authors | Main Method | Secondary Method (s) |
|---|---|---|
| Queiroz C, Mahmood A Tari Z (2013) [4] | Bayesian networks | N/A |
| Cerotti D, et al. (2019) [34] | Bayesian networks | Attack graph |
| Cerroti D, et al. (2020) [35] | Dynamic Bayesian networks | Attack graph |
| Giorgio A D Liberati F. (2011) [25] | Dynamic Bayesian networks | N/A |
| Elmrabit N, et al. (2020) [31] | Bayesian networks | N/A |
| Gaber A, Seddik G K, and Elezabi A Y. (2015) [55] | Bayesian methodology | Neyman–Pearson forms |
| Gaskova D A Massel A G. (2019) [36] | Bayesian network | Dynamic cognitive maps |
| Hossain N U I, et al. (2020) [9] | Bayesian networks | N/A |
| Le A, et al. (2019) [6] | Bayesian networks | Factor Analysis of Information Risk Loss Event Frequency (FAIR LEF) |
| Liu X, et al. (2021) [7] | Bayesian attack-defence game model | Refined Bayesian Nash equilibrium |
| Bode M A, et al. (2015) [33] | Bayesian networks | N/A |
| Rana M M, Bo R Abdelhadi. (2020) [56] | Bayesian networks | Optimal filter theory Graph theory |
| Marrone S, et al. (2015) [38] | Bayesian networks | Petri nets |
| Li S, et al. (2018) [39] | Hybrid Bayesian risk graph (HBRG) | Hidden Markov model |
| Sahu A Davis K. (2021) [57] | Bayesian attack graphs | Machine-based structured learning |
| Drago V, et al. (2019) [13] | Bayesian networks | N/A |
| Lyu X, Ding Y Yang S H. (2020) [26] | Bayesian networks | N/A |
| Wang P, et al. (2018) [30] | Bayesian networks | Attack graphs |
| Drago A, et al. (2013) [27] | Two-layered Bayesian networks | N/A |
| Yeboah-Ofori A, et al. (2019) [32] | Bayesian belief network | N/A |
| M Smith M Pate-Cornell (2017) [59] | Bayesian-adaptive multi-armed bandits | N/A |
| J Milanovic W Zhu (2017) [60] | Complex network theory | N/A |
| Caviglione L Coccoli M (2020) [29] | Identification and classification Model-driven design | N/A |
| Djigal H, Jun F Lu J. (2017) [17] | Zero-Knowledge Protocol using Elliptic Curve Discrete Logarithm Problem | N/A |
| Zografopoulos I, Ospina J, Konstantinou C. (2020) [2] | Typical holistic risk assessment framework | N/A |
| Behl M Mangharam R. (2016) [40] | Regression trees-based models | N/A |
| Wang P, Ali A Kelly W. (2015) [24] | Typical threat modelling methodology | N/A |
| Zhu W Milanovic J V. (2017) [41] | Weighted complex network theory | N/A |

#### 5.2.4. Model Complexity

The models regarding threat modelling break down the SCI systems into much smaller and measurable chunks throughout the methodological process. Model to model with what attributes can be focused on and expanded on into the smaller aspect, which can then provide those values to effectively introduce bespoke cyber-security mechanisms within the CPS. It depends upon whether the methodology takes a high- or low-level review, which is very dependent on the objectives regarding the scope of the system or previously identified weaknesses where bespoke threat modelling methodologies could be developed. There is a need, however, for more high-level methodologies which review not only the intricacies regarding the ToE but also the larger perspective when malicious actions affect the SCI to where else on the smart grid, both the local and global levels.

**Table 3.** A collection of the different metrics that are used by the reviewed literature, collected to show an array associated across them.

| ***Reactive Restoration*** | ***Physical Proactive Countermeasures*** |
|---|---|
| Survivability, Information diversity score, Service state, Interdependencies, Heterogeneity, Stability, Recoverability, Resilience, Redundancy. | Monitoring, Atomic events, Boundary values, Constraints, Intentions, Impact, System performance, Scalability, Physical layer, Field control layer, Learner space, Data space, Infrastructure space, Security policy, Predictive value, Electrical distance, Risk. |
| ***Cyber Proactive Countermeasures*** | ***Threat Characteristics*** |
| Network traffic, Communication-layer, Monitoring, Offline diagnosis (smoothing), Reporting, Propagation level, Service layers, Bad data, Detector decision, Hypothesis, Cost value (non-financial), Concepts, types, Boundary values, Sensitivity analysis, factors, sub-factors, Vulnerability, Control strength, Constraints, Intentions, Impact, System performance, vulnerability, Alerts, Scalability, Data dependency, Time complexity, Accuracy, Precision, Interpretation, Simplicity, Expressiveness, Definiteness of state, Evidence impact, Process monitoring layer, Enterprise management layer, Services, Learner space, Data space, Infrastructure space, Loc/Glob-Storage, Data processing, Security policy, Resources, Leaf support, Predictive value, Confidence, Threat intelligence, Vulnerable-Weighted, Risk, Link direction. | Attack capabilities, Prediction, Probability, Severity, Loss event frequency, Attack techniques, Threat capabilities, End goal, Attack mission, Type, Attack sequence, General, Specific, Impairment, Action, Weight adjustment, CVSS.<br><br>— Insider Threat Exclusive —<br>Technical factors, Organisational factors, Human factors, Risk, User profiles, Keywords, Behaviour, Influences. |

#### 5.2.5. Modelling Interdependencies

Interdependency plays a big part of CNI, regarding each of the different sectors having both a relationship between sectors and sub-sectors. Some of the reviewed methodologies [4,9,23,25,41,61] discuss and analyse the causal relationships of the ToEd system within a range of different levels regarding how cascading effects influence the system throughout and the depth of which these casual relationships are understood. Dynamic techniques are also heavily important regarding interdependency as these influences need to be fully understood over a specific time scale, and the best process to truly capture systematic resilience is under negative action pressure. Methodologies that lack mention of CII suffer from a lack of providing a complete or overall security analysis within their ToE, based around impact and influences being one of the major aspects regarding system states within CPSs. Previous methodologies should develop and review their process for understanding these systems, including the effect of states, metrics, and transitional relationships also can be used to MaS threat proportions through the model. Please see Table 4

#### 5.2.6. Applicable Bayesian-Based Smart City Environments

The environment where threat modelling methodologies aim to MaS SCI for cybersecurity focus around a single infrastructure, which can, in turn, dictate the complexity of the methodologies. A graphical modelling approach to dismantle the CPSs into multiple layers [41], to display the interconnected systems into distinctive physical objects, cyber objects, and communication data across these two systems. In contrast, Bayesian-based approaches functionally and visually form these objects across an overlapping complete model [9]. The interconnected digital environment that SCI fosters, where this SoSs provide the basis for the overall cyber ecosystem. BNs modelling of these relationships is effective within this environment through connecting the objectives by objects, relationships, and valued weightings to each model feature with some distinctive categorised breakdown.

**Table 4.** A summary of the differently reviewed methodologies demonstration datasets to highlight their theoretical process and to validate their application viability.

| Authors | Validation Method | Secondary Method (s) |
|---|---|---|
| Queiroz C, Mahmood A Tari Z (2013) [4] | Simulation | N/A |
| Cerotti D, et al. (2019) [34] | Case study | N/A |
| Cerroti D, et al. (2020) [35] | Case study | Expert opinion |
| Giorgio A D Liberati F. (2011) [25] | Case study | N/A |
| Elmrabit N, et al. (2020) [31] | Case study | Expert opinion |
| Gaber A, Seddik G K, and Elezabi A Y. (2015) [55] | Case study | N/A |
| Gaskova D A Massel A G. (2019) [36] | Example demonstration | N/A |
| Hossain N U I, et al. (2020) [9] | Case study | Expert opinion |
| Le A, et al. (2019) [6] | Experiment | Expert opinion |
| Liu X, et al. (2021) [7] | Case study | N/A |
| Bode M A, et al. (2015) [33] | Experiment | N/A |
| Rana M M, Bo R Abdelhadi. (2020) [56] | Simulation | N/A |
| Marrone S, et al. (2015) [38] | Case study | N/A |
| Li S, et al. (2018) [39] | Experiment | N/A |
| Sahu A Davis K. (2021) [57] | Experiment | N/A |
| Drago V, et al. (2019) [37] | Case study | Expert models |
| Lyu X, Ding Y Yang S H. (2020) [26] | Case study | Expert opinions |
| Wang P, et al. (2018) [30] | Experiment | N/A |
| Drago A, et al. (2013) [27] | Experiment | N/A |
| Yeboah-Ofori A, et al. (2019) [32] | Case study | N/A |
| M Smith & M Pate-Cornell (2017) [59] | Case study | N/A |
| J Milanovic & W Zhu (2017) [60] | Case study | N/A |
| Caviglione L & Coccoli M (2020) [29] | Toy example | N/A |
| Djigal H, Jun F Lu J. (2017) [17] | Simulation cases | N/A |
| Zografopoulos I, Ospina J, and Konstantinou C. (2021) [2] | Case study | N/A |
| Behl M Mangharam R. (2016) [40] | Case study | N/A |
| Wang P, Ali A Kelly W. (2015) [24] | Experiment | N/A |
| Zhu W Milanovic J V. (2017) [41] | Experiment | N/A |

### *5.3. Overview of the Systematic Literature Review*

#### 5.3.1. Towards an Effective Solution

An overview of the different metrics used within these articles highlights the wide range of threat modelling variation even within Bayesian-based approaches and the associated metrics to conclude their analysis. The metrics are reviewed in four categories: reactive, physical, cyber, and threat capabilities. With these identified, they could be integrated into existing or newly created methodologies, demonstrated in some of the reviewed methodologies, highlighting future research avenues that should be pursued. One example is Gaber et al. [55] through hypothesis error detection, both a more accurate structure to threat model SCI, and different situations through its application can be analysed. Another is Drago et al. [27] following a multi-layered Bayesian approach using CPS model through CIP_VAM ULM then BNs to probabilistic relationships within the system. Finally, other methodologies use an integration of two different modelling to assist in providing a com-

prehensive model [38]. These different approaches provide the most MaS methodologies comparatively within the reviewed literature and help narrow down the best possible modelling framework approaches to understanding the complex nature regarded within SCI. The result of this is to highlight the need for standardisation across the board for MaS of smart technologies surrounding critical services to bring together all aspects.

#### 5.3.2. Smart City Environment Overview

The environment for SCI cyber-security stretches across three distinctive layers for cyber, physical, and human elements that share interdependency relationships across selectively associated metrics. Mostly there is a focus on the cyber, physical, and CPS systems and interconnected relationships and the human elements, which are uselessly modelled to influence the evaluated system. Examples of distinctive methodologies are Hossain et al. [9] for CPS focus and Elmrabit et al. [31] for human-focused elements. The core issue regarding this is that human elements also interplay individually with the cyber and physical, where future methodologies need to analyse and MaS the interplay between them. With this in mind, there is an overall lack of national level perspective analysis regarding SCI and related CNI to analyse and provide complete protective mechanisms fully. These systems are already complex across cyber-physical technical layers; modelling should also include local, regional, and national influences on the overall system structure's effectiveness and importance regarding the much larger national architecture.

Validation will require practical application in regards to their ToEd system to release these and to understand how it fits within the web of relationships across cyber, physical, and human influential complements. Very few of the methodologies discussed here go any further than expert opinion in addition to the mathematical checking regarding the logic of the proposed MaS methodologies. Testing these networks through live systems is the next key milestone across different CNI systems regarding the same type, within a relational context across other interdependent systems from a national CII perspective. SCI and related CNI take validation of the methods further, with the requirement of operating across multiple different individual systems and handling their characteristics—both older and newer infrastructures making up the overall national grid. The MaS methods will need to be developed and tested across a range of differently implemented architectures to provide an acceptable level of maturity towards practicality for addressing challenges and issues, especially representative across IoT devices present within SCI. Please see Table 5 for an overview of the different reviewed threat modelling methodologies.

**Table 5.** Comparison of different threat modelling methodologies.

| Author | Methodology Application | Main Method | Sec. Method (s) | Threat Actor Type | Test Data Method | Validation | Key Metrics |
|---|---|---|---|---|---|---|---|
| Queiroz C, Mahmood A, and Tari Z. (2013) [4] | Predicting probabilistic survivability model for SCADA systems. | Bayesian networks | N/A | SCADA-focused cyber-attacks | Simulation | <<< | Information diversity score, survivability, service states, network traffic. |
| Cerotti D, et al. (2019) [34] | Framework to analyze and detect the smart grid infrastructure (also industrial control systems) | Bayesian networks | Attack graph | Predictive and diagnostic analysis | Case study | <<< | Attack capabilities, dependencies, communication. |
| Cerotti D, et al. (2020) [35] | Understanding cyber-security for distributed energy plants for both casual and temporal time. | Dynamic Bayesian networks | Attack graph | Predictive and diagnostic analysis of threat dependencies | Case study | Expert opinions | Monitoring, prediction, offline diagnosis, reporting messages. |
| Giorgio A D and Liberati F. (2011) [25] | Analyzing the different layers of critical infrastructure interdependency for modelling and simulation analysis. | Dynamic Bayesian networks | N/A | Analysis of critical infrastructure interdependencies | Case study | <<< | atomic events, propagation, services layers. |
| Elmrabit N, et al. (2020) [31] | Proactive insider risk predictive analysis framework for technical and non-technical threats. | Bayesian networks | N/A | Insider threat risk prediction | Case study | Expert opinions | Technical factors, organizational factors, human factors, risk level. |
| Gaber A, Seddik G K, and Elezabi A Y. (2015) [55] | Threat modelling methodology with joint estimation-detection for cyber-attacks towards the smart grid. | Bayesian methodology | Neyman-Pearson forms | Cyber-attacks in the smart grid | Case study | <<< | Bad data, detector decision, hypothesis, probability, cost value. |
| Gaskova D A and Massel A G. (2019) [36] | Relationship modelling methodology of cyber-threats towards the energy sector. | Bayesian network | Dynamic cognitive maps | Cyber-attacks in the smart grid | Example demonstration | <<< | Concepts, type, boundary values, pre-crisis/crisis. |
| Hossain N U I, et al. (2020) [9] | Modelling cyber-security within the smart grid system of systems for characteristics of resilience, vulnerability, and restoration. | Bayesian networks | N/A | Cyber-attacks in the smart grid | Case study | Expert opinion | Sensitivity analysis, resilience, factors and sub-factors, recoverability. |
| Le A, et al. (2019) [6] | Smart grid cyber-threat framework using analysis of information risk to identify cyber-security attacks. | Bayesian network | Factor Analysis of Information Risk Loss Event Frequency (FAIR LEF) | Cyber-attacks in the smart grid | Experiment | Expert opinion | Threat severity, vulnerability, event frequency, control strength. |
| Liu X, et al. (2021) [7] | Quantitative cyber-physical security analysis methodology for industrial control systems. | Bayesian attack-defense game model | Refined Bayesian Nash equilibrium | Cyber-attacks in the smart grid | Case study | <<< | Attack techniques, threat capabilities, end goal, |
| Bode M A, et al. (2015) [33] | Cyber situation awareness risk analysis through probability risk matrixes to identify key attack attributes. | Bayesian networks | N/A | Cyber situational awareness risk analysis | Experiment | <<< | Attack mission, constraints, capabilities, intentions, impact, types. |

**Table 5.** *Cont.*

| Author | Methodology Application | Main Method | Sec. Method (s) | Threat Actor Type | Test Data Method | Validation | Key Metrics |
|---|---|---|---|---|---|---|---|
| Rana M M, Bo R and Abdelhadi. (2020) [56] | Threat modelling methodology for distributed grid dynamic state estimation algorithm. | Bayesian networks | Optimal filter theory Graph theory | Cyber-attacks in the smart grid | Simulation | <<< | Resilience, false data, attack sequence |
| Marrone S, et al. (2015) [38] | Modelling methodology for both cyber and physical security vulnerability assessment railway system infrastructure. | Bayesian networks | Petri nets | Cyber and physical modelling of railway systems | Case study | <<< | System performance, vulnerability. |
| Li S, et al. (2018) [39] | Proposed dynamic security risk evaluation framework for cyber-physical systems to analyse attack activity patterns and risk propagations cross layer. | Hybrid Bayesian risk graph (HBRG) | Hidden Markov model | Cyber-attacks on cyber-physical social-based systems | Experiment | <<< | Attack types, user profiles, keywords, behaviour, influences. |
| Sahu A and Davis K. (2021) [57] | Attack graph machine learning techniques to understand cyber-physical power architecture evaluated score-based modelling and simulation. | Bayesian attack graphs | Machine-based structured learning | Cyber-attacks in the smart grid | Experiment | <<< | Alerts, scalability, data dependency, time complexity, accuracy. |
| Drago V, et al. (2019) [37] | Applying entropy metrics to assess uncertainty with the purpose of cyber threats detections. | Bayesian networks | N/A | Uncertainty analysis of cyber-attacks | Case study | Expert models | Accuracy, precision, interpretation, simplicity, expressiveness, definiteness of state, evidence impact. |
| Lyu X, Ding Y and Yang S H. (2020) [26] | Hierarchical identify cyber-to-physical risk assessment for cyber-physical systems to identify impacts on physical process safety. | Bayesian networks | N/A | Cyber-attacks at cyber-physical systems | Case study | Expert opinions | Physical, field control, process monitor, enterprise management. |
| Wang P, et al. (2018) [30] | Relationship framework for understanding cyber-security to classify and attacks into groups and specialized variety. | Bayesian networks | Attack graphs | Cyber attack inference | Experiment | <<< | General threat, specific threat, vulnerability, capabilities, |
| Drago A, et al. (2013) [27] | Model-driven distributed vulnerability methodology towards complex railway network cyber-physical systems. | Two-layered Bayesian networks | N/A | Cyber and physical | Experiment | <<< | Threat, service, system, attack, protection, impairment, action, object. |
| Yeboah-Ofori A, et al. (2019) [32] | Detecting supply chain attacks on cyber-physical systems through Bayesian belief networks. | Bayesian belief network | N/A | Cyber and physical | Case study | <<< | Malware propagation characteristics, attacker data, cybercrime type manipulation |
| M Smith and M Pate-Cornell (2017) [59] | Cyber risk analysis for the smart grid using multi-armed bandit approach | Bayesian-adaptive multi-armed bandits | N/A | Cyber and physical | Case study | <<< | Defensive value, optimal allocation, finance, Time remaining |
| J Milanovic W Zhu (2017) [60] | Modelling interconnected critical infrastructure using three dimensional complex network theory | Complex network theory | N/A | Cyber and physical | Case study | <<< | Adjacency matrix, node degree, path length and geodesics, betweenness centrality, efficiency. |

**Table 5.** *Cont.*

| Author | Methodology Application | Main Method | Sec. Method (s) | Threat Actor Type | Test Data Method | Validation | Key Metrics |
|---|---|---|---|---|---|---|---|
| Caviglione L and Coccoli M. (2020) [29] | Holistic model for cyber-security e-learning towards smart city infrastructure across three homogenous groups to classify threats and vulnerabilities. | Identification and classification Model-driven design | N/A | Cyber-security learning for smart cities. | Toy example | <<< | Learner space, data space, infrastructure space, attack type. |
| Djigal H, Jun F and Lu J. (2017) [17] | Secure framework called "SEFSCITY" for smart city infrastructure development governance surrounding key aspects. | Zero-Knowledge Protocol using Elliptic Curve Discrete Logarithm Problem | N/A | Threat modelling for smart cities | Simulation cases | <<< | Loc-storage, glob-storage, data processing, security policy. |
| Zografopoulos I, Ospina J, and Konstantinou C. (2021) [2] | Overview literature review for the cyber-physical security within the energy sector environment. | Typical holistic risk assessment framework | N/A | Cyber-attacks in the smart grid | Case study | <<< | Resources, frequency stability, time, packets |
| Behl M and Mangharam R. (2016) [40] | Reviewing different interactive analytic smart cities infrastructure for key metrics and evaluated systems. | Regression trees-based models | N/A | Threat modelling for smart cities | Case study | <<< | Leaf support, predicted value, confidence. |
| Wang P, Ali A, and Kelly W. (2015) [24] | Threat modelling methodologies for smart city infrastructure for data security and identification of threats. | Typical threat modelling methodology | N/A | Data security and threat modelling smart cities | Experiment | <<< | Threat value, threat weight, threat factor, weight adjustment, CVSS scores, threat intelligence. |
| Zhu W and Milanovic J V. (2017) [41] | Modelling of cyber-physical systems infrastructure interdependencies using weighted system and three-dimensioned approach. | Weighted complex network theory | N/A | Analysis of critical infrastructure interdependencies | Experiment | <<< | Distance, vulnerability-weighted, link direction, risk. |

Distinctively all reviewed MaS SCI are focused on being applied towards the primary larger focus surrounding modelling and frameworks for securing energy sector smart grid implementations. Others are lacking review, specifically through BN-based methodologies which could provide a solution to other important sectors with the challenges faced across smart functionalities of healthcare, emergency response, and transportation which make up smart cities. Additional research across both identifications of metrics and MaS cyber threats against the system to improve the security posture of key critical smart city systems should be high up on the priority and follow similar depth to how these reviewed methodologies are. Furthermore, there should be a push towards MaS reviewing aspects similar to the smart grid from the national perspective because the interconnected systems of systems between them were much larger perspectives. Most of the research focuses on the local area, where individual systems are located, but there is a lack of research surrounding the much larger collective of SCI with interlinked CNI. Many of the different CNIs comprise the services that smart cities use and both interconnections across both industrial systems and the end users of the CNI.

## 6. Conclusions

Cyber-security is a critical aspect within the newly developing smart sector, with a high priority towards maintaining research goals. A SLR is conducted towards Bayesian-based threat modelling of SCI literature to further development of future proposed methodologies—a total of 55 articles were reviewed throughout this process, in regards to the search strings used. An array of alternative methodologies are also examined to build upon the different techniques and metrics used to understand the risks, vulnerabilities, and threats associated with these complex systems—these are threat modelling methodologies. Each article was dissected into eight distinctive categories for cross-examination regarding proposed methodologies, breaking them down into used techniques, metrics identified, and testing/validation process. The framework they reviewed provides a comparison regarding the wide array of differences in threat MaS approaches, with both looking into, primarily, BN and a few alternative options. The alternatives reviewed provided an overview of other methodologies following non-Bayesian approaches to improve understanding of current threat modelling literature, highlighting the different techniques and unique twists that proposed methodologies can utilise. These options could also be used in conjunction with Bayesian-based approaches to help bolster cyber-security posture regarding SCI ToEs. The overview regarding smart city threat modelling is that it remains a brand-new area of research where most models are still only validated through application into theoretical MaSs. Therefore, one of the biggest pursuits would be to apply these methodologies within a live system to check the practical applications and provide real-life data that could be used to expand upon the applied solution. This level of understanding can still be gained through small or medium level infrastructures, with an alternative option being enterprise architectures that share similar systematic characteristics of SCI CPSs.

## 7. Future Research

Two of the most important aspects of these systems that need future research within the wider context is examining and modelling CII. BN CII modelling is a very effective technique with casual modelling which can be seen within proposed methodologies [9,25], represented through utilisation of DBN towards the ToE. The other is that identified metrics regarding SCI share similar levels of complexity and quantity. Selection, influences, and valuation of these are core to understanding threat modelling and providing pragmatic solutions, where future progress could be aimed at further exploration into the interdependency and appraisement for metrics of the reviewed methodologies. Other notable takeaways within the research sphere are a further review identifying additional issues and challenges that SCI faces, as this will be a constantly ongoing process throughout the evolution of smart technologies. A better understanding could be reached for these systems, allowing for higher accuracy and prediction within proposed threat models, through improvements by expanding either current methodologies towards better handling the

complexities within SCI, through adopting multi-layered and technique approaches. Future methodologies need to make sure they comprise their ToE across physical, cyber, and communication layers between each other, alongside an interdependency analysis regarding the individual nodes' influential factors to handle systematic relationships. A future proposal through research could be a three-layered multi-methodological approach applied across the individual system analysis, influence interdependencies, threat propagation, and impacts. Further research will use three different methodologies to compensate for any weaknesses across the other techniques used. A key aspect of this approach is the interconnection between the different layers and the metrics conversation regarding the different techniques applied to the systematic model.

**Author Contributions:** Supervision, H.C. and T.V.; Writing—original draft, M.W.; Writing—review and editing, M.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The author declares no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| BN | Bayesian networks |
| DBN | Dynamic Bayesian networks |
| DAG | Directed acyclic graph |
| CNI | Critical national infrastructure |
| CII | Critical infrastructure interdependency |
| CLGD | conditional linear Gaussian distributions |
| SLR | Systematic literature review |
| SCI | Smart city infrastructure |
| CF | Cascading failures |
| CPS | Cyber-physical system |
| IoT | Internet of things |
| URREF | Uncertainty representation and reasoning evaluation framework |
| CPT | Conditional probability table |
| ToE | Target of evaluation |
| SCADA | supervisory control and data acquisition |
| MaS | Modelling and simulation |
| AT | Attack graph |
| NPF | Neyman-Pearson forms |
| DCM | Dynamic cognitive maps |
| FAIR LEF | Factor analysis of information risk loss event frequency |
| RBNE | Refined Bayesian Nash equilibrium |
| OFTGT | Optimal filter theory graph theory |
| PN | Petri net |
| HMM | Hidden Markov model |
| MBSL | Machine-based structured learning |
| ICTS | Information communication technology system |
| TLBN | Two-layered Bayesian network |
| ICMDD | Identification and classification model-driven design |
| ZKPECDLP | Zero-knowledge protocol using elliptic curve discrete logarithm problem |
| RTBM | Regression tree-based model |
| TTMM | Typical threat modelling methodology |
| WCNT | Weighted complex network theory |

## References


1. Simon, T. Critical Infrastructure and the Internet of Things. *Pap. Ser. No* **2017**, *46*, 1–20.
2. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
3. Selin, J. Evaluation of Threat Modeling Methodologies: A Case Study. Master's Thesis, JAMK University of Applied Science, School of Technology Information and Communication Technology, Degree-Granting University, Chicago, IL, USA, 2019.
4. Queiroz, C.; Mahmood, A.; Tari, Z. A Probabilistic Model to Predict the Survivability of SCADA Systems. *IEEE Trans. Ind. Informatics* **2013**, *9*, 1975–1985. [CrossRef]
5. Zhou, Y.; Zhu, C.; Tang, L.; Zhang, W.; Wang, P. Cyber Security Inference Based on a Two-Level Bayesian Network Framework. In Proceedings of the 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 7–10 October 2018; pp. 3932–3937. [CrossRef]
6. Le, A.; Chen, Y.; Chai, K.K.; Vasenev, A.; Montoya, L. Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats. *Mob. Netw. Appl.* **2019**, *24*, 1713–1721. [CrossRef]
7. Liu, X.; Zhang, J.; Zhu, P.; Tan, Q.; Yin, W. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Comput. Secur.* **2021**, *102*, 102138. [CrossRef]
8. Chockalingam, S.; Pieters, W.; Teixeira, A.; van Gelder, P. Bayesian network models in cyber security: A systematic review. *Lect. Notes Comput. Sci.* **2017**, *10674*, 105–122. [CrossRef]
9. Hossain, N.U.I.; Nagahi, M.; Jaradat, R.; Shah, C.; Buchanan, R.; Hamilton, M. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *J. Comput. Des. Eng.* **2020**, *7*, 352–366. [CrossRef]
10. Franke, U.; Brynielsson, J. Cyber situational awareness - A systematic review of the literature. *Comput. Secur.* **2014**, *46*, 18–31. [CrossRef]
11. Hamid, B.; Jhanjhi, N.; Humayun, M.; Khan, A.; Alsayat, A. Cyber Security Issues and Challenges for Smart Cities: A survey. In Proceedings of the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 14–15 December 2019. [CrossRef]
12. Colding, J.; Barthel, S. An urban ecology critique on the "Smart City" model. *J. Clean. Prod.* **2017**, *164*, 95–101. [CrossRef]
13. Dragos, V.; Ziegler, J.; De Villiers, J.P.; De Waal, A.; Jousselme, A.L.; Blasch, E. Entropy-Based Metrics for URREF Criteria to Assess Uncertainty in Bayesian Networks for Cyber Threat Detection. In Proceedings of the 2019 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, 2–5 July 2019.
14. Ahad, M.A.; Paiva, S.; Tripathi, G.; Feroz, N. Enabling technologies and sustainable smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102301. [CrossRef]
15. Infrastructure Interdependencies and Resilience. In *Chile Earthquake of 2010*; American Society of Civil Engineers: Reston, VA, USA, 2013; Volume 37, pp. 365–386. [CrossRef]
16. Chourabi, H.; Nam, T.; Walker, S.; Gil-Garcia, J.R.; Mellouli, S.; Nahon, K.; Pardo, T.A.; Scholl, H.J. Understanding smart cities: An integrative framework. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2289–2297. [CrossRef]
17. Djigal, H.; Jun, F.; Lu, J. Secure Framework for Future Smart City. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 76–83. [CrossRef]
18. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report 2.3; Keele University: Keele, UK, 2007.
19. Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.C.; Regnell, B.; Wesslén, A. *Experimentation in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2012; p. 259. [CrossRef]
20. Social Science Research Unit. EPPI-Reviewer. 2021. Available online: https://eppi.ioe.ac.uk/cms/Default.aspx?tabid=2914 (accessed on 14 November 2021).
21. Curt, C.; Tacnet, J.M. Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Anal.* **2018**, *38*, 2441–2458. [CrossRef] [PubMed]
22. Kalinin, M.; Krundyshev, V.; Zegzhda, P. Cybersecurity risk assessment in smart city infrastructures. *Machines* **2021**, *9*, 78. [CrossRef]
23. Hadjsaid, N.; Tranchita, C.; Rozel, B.; Viziteu, M.G.; Caire, R. Modeling cyber and physical interdependencies—Application in ICT and power grids. In Proceedings of the 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–6. [CrossRef]
24. Wang, P.; Ali, A.; Kelly, W. Data security and threat modeling for smart city infrastructure. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015. [CrossRef]
25. Di Giorgio, A.; Liberati, F. Interdependency modeling and analysis of critical infrastructures based on Dynamic Bayesian Networks. In Proceedings of the 2011 19th Mediterranean Conference on Control & Automation (MED), Corfu, Greece, 20–23 June 2011; pp. 791–797. [CrossRef]
26. Lyu, X.; Ding, Y.; Yang, S.H. Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems. *IEEE Access* **2020**, *8*, 88506–88517. [CrossRef]

27. Drago, A.; Marrone, S.; Mazzocca, N.; Tedesco, A.; Vittorini, V. Model-driven estimation of distributed vulnerability in complex railway networks. In Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mare, Italy, 18–21 December 2013; pp. 380–387. [CrossRef]
28. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
29. Caviglione, L.; Coccoli, M. A holistic model for security of learning applications in smart cities. *J. E-Learn. Knowl. Soc.* **2020**, *16*, 1–10. [CrossRef]
30. Wang, W.; Yang, S.; Hu, F.; Stanley, H.E.; He, S.; Shi, M. An approach for cascading effects within critical infrastructure systems. *Phys. A Stat. Mech. Its Appl.* **2018**, *510*, 164–177. [CrossRef]
31. Elmrabit, N.; Yang, S.H.; Yang, L.; Zhou, H. Insider Threat Risk Prediction based on Bayesian Network. *Comput. Secur.* **2020**, *96*, 101908. [CrossRef]
32. Yeboah-Ofori, A.; Islam, S.; Brimicombe, A. Detecting cyber supply chain attacks on cyber physical systems using bayesian belief network. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; pp. 37–42. [CrossRef]
33. Bode, M.A.; Oluwadare, S.A.; Alese, B.K.; Thompson, A.F.B. Risk analysis in cyber situation awareness using Bayesian approach. In Proceedings of the 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, 8–9 June 2015. [CrossRef]
34. Cerotti, D.; Codetta-Raiteri, D.; Egidi, L.; Franceschinis, G.; Portinale, L.; Dondossola, G.; Terruggia, R. Analysis and Detection of Cyber Attack Processes targeting Smart Grids. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, 29 September–2 October 2019. [CrossRef]
35. Cerotti, D.; Codetta-Raiteri, D.; Dondossola, G.; Egidi, L.; Franceschinis, G.; Portinale, L.; Terruggia, R. Evidence-based analysis of cyber attacks to security monitored distributed energy resources. *Appl. Sci.* **2020**, *10*, 4725. [CrossRef]
36. Gaskova, D.; Massel, A. Semantic modeling of cyber threats in the energy sector using Dynamic Cognitive Maps and Bayesian Belief Network. *Adv. Intell. Syst. Res.* **2019**, *166*, 326–329. [CrossRef]
37. Drago, A.; Marrone, S.; Mazzocca, N.; Nardone, R.; Tedesco, A.; Vittorini, V. A model-driven approach for vulnerability evaluation of modern physical protection systems. *Softw. Syst. Model.* **2019**, *18*, 523–556. [CrossRef]
38. Marrone, S.; Rodríguez, R.J.; Nardone, R.; Flammini, F.; Vittorini, V. On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. *Comput. Electr. Eng.* **2015**, *47*, 275–285. [CrossRef]
39. Li, S.; Zhao, S.; Yuan, Y.; Sun, Q.; Zhang, K. Dynamic Security Risk Evaluation via Hybrid Bayesian Risk Graph in Cyber-Physical Social Systems. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 1133–1141. [CrossRef]
40. Behl, M.; Mangharam, R. Interactive analytics for smart cities infrastructures. In Proceedings of the 2016 1st International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE) in partnership with Global City Teams Challenge (GCTC) (SCOPE-GCTC), Vienna, Austria, 11 April 2016; pp. 1–6. [CrossRef]
41. Zhu, W.; Milanovic, J.V. Interdepedency modeling of cyber-physical systems using a weighted complex network approach. In Proceedings of the 2017 IEEE Manchester PowerTech, Manchester, UK, 18–22 June 2017. [CrossRef]
42. Tajer, A.; Kar, S.; Poor, H.V.; Cui, S. Distributed joint cyber attack detection and state recovery in smart grids. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 202–207. [CrossRef]
43. Ahmadi-Assalemi, G.; Al-Khateeb, H.; Epiphaniou, G.; Maple, C. Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review. *Smart Cities* **2020**, *3*, 894–927. [CrossRef]
44. House of Lords; House of Commons. *Joint Committee on the National Security Strategy Cyber Security Skills and the UK's Critical National Infrastructure: Government Response to the Committee's Second Report of Session 2017–2019 Second Special Report of Session*; House of Lords: London, UK, 2018; p. 64.
45. Luiijf, H.A.; Besseling, K.; Spoelstra, M.; De Graaf, P. Ten national cyber security strategies: A comparison. *Lect. Notes Comput. Sci.* **2013**, *6983*, 1–17. [CrossRef]
46. UK Trade & Investment. Smart Cities Pitchbook. In *Technology is Great, Britian & Northern Ireland*; Old Admiralty Building: London, UK, 2016; p. 49.
47. Knapp, E. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems*; Syngress: Waltham, MA, USA, 2011; pp. 1–341. [CrossRef]
48. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25. [CrossRef]
49. Rinaldi, S.M. Modeling and simulating critical infrastructures and their interdependencies. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004; Volume 37, pp. 873–880. [CrossRef]
50. Alcaraz, C. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2017**, *8*, 53–66. [CrossRef]
51. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 26–29 September 2017; pp. 1–6. [CrossRef]

52. Dudenhoeffer, D.D.; Permann, M.R.; Manic, M. CIMS: A framework for infrastructure interdependency modeling and analysis. In Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, USA, 3–6 December 2006; pp. 478–485. [CrossRef]
53. St. John-Green, M.; Watson, T. Safety and Security of the Smart City—When our infrastructure goes online. In Proceedings of the 9th IET International Conference on System Safety and Cyber Security (2014), Manchester, UK, 15–16 October 2014; pp. 1–6. [CrossRef]
54. Burmester, M.; Magkos, E.; Chrissikopoulos, V. Modeling security in cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 118–126. [CrossRef]
55. Gaber, A.; Seddik, K.G.; Elezabi, A.Y. Joint estimation-detection of cyber attacks in smart grids: Bayesian and non-Bayesian formulations. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 2245–2250. [CrossRef]
56. Rana, M.M.; Bo, R.; Abdelhadi, A. Distributed Grid State Estimation under Cyber Attacks Using Optimal Filter and Bayesian Approach. *IEEE Syst. J.* **2021**, *15*, 1970–1978. [CrossRef]
57. Sahu, A.; Davis, K. Structural Learning Techniques for Bayesian Attack Graphs in Cyber Physical Power Systems. In Proceedings of the 2021 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. [CrossRef]
58. Graja, I.; Kallel, S.; Guermouche, N.; Cheikhrouhou, S.; Hadj Kacem, A. A comprehensive survey on modeling of cyber-physical systems. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e4850. [CrossRef]
59. Smith, M.; Paté-Cornell, E. Cyber Risk Analysis for a Smart Grid: How Smart Is Smart Enough? A Multi-Armed Bandit Approach. In *A Systems Approach to Cyber Security*; IOS Press: Amsterdam, The Netherlands, 2017; pp. 37–56.
60. Milanović, J.V.; Zhu, W. Modeling of interconnected critical infrastructure systems using complex network theory. *IEEE Trans. Smart Grid* **2017**, *9*, 4637–4648. [CrossRef]
61. Boyes, H.; Isbell, R.; Watson, T. Critical Infrastructure in the Future City Developing Secure and Resilient Cyber–Physical Systems. In Proceedings of the 9th International Conference, CRITIS 2014, Limassol, Cyprus, 13–15 October 2014; pp. 13–15.