Research Technical Report
April 2019

# Critical Infrastructure Protection Approaches

## Analytical Outlook on Capacity Responsiveness to Dynamic Trends

Jeremy M Watson CBE, Uchenna D Ani

PETRAS
INTERNET OF THINGS RESEARCH HUB

Analytical Lenses for Internet of Things Threats
(ALIoTT)

PETRAS

UCL
DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

**Details of document preparation and issue:**

| Version no. | Prepared | Checked | Reviewed | Approved | Issue date | Issue status |
|---|---|---|---|---|---|---|
| 1.1 | Uchenna D Ani | | - | - | 21/07/18 | 1st Draft |
| 1.2 | Uchenna D Ani | Jeremy Watson | Jason Nurse | Jeremy Watson | 13/09/18 | 2nd Draft |
| 1.3 | Jeremy Watson & Uchenna D Ani | Uchenna D Ani | Jeremy Watson | Jeremy Watson | 23/11/18 | 3rd Draft |
| 1.4 | Uchenna D Ani | Uchenna D Ani | Jeremy Watson | Jeremy Watson | 8/01/19 | Final Version |

# Contents

EXECUTIVE SUMMARY ..... V
1. INTRODUCTION ..... 1
1.1 BACKGROUND ..... 1
1.2 NEED FOR COMPARATIVE SURVEY ..... 1
1.3 RESEARCH QUESTIONS ..... 2
2. METHODOLOGY ..... 2
2.1 LITERATURE GATHERING ..... 2
3. CRITERIA FOR COMPARATIVE EVALUATION OF CIP APPROACHES ..... 3
3.1 SECTORS OF CRITICAL INFRASTRUCTURE (CI) ..... 3
3.2 MODELLING TECHNIQUES FOR CIS ..... 4
3.2.1 AGENT-BASED ..... 5
3.2.2 SYSTEM DYNAMICS-BASED ..... 5
3.2.3 EMPIRICAL-BASED ..... 5
3.2.4 NETWORK-BASED ..... 5
3.2.5 ECONOMICS-BASED ..... 6
3.2.6 OTHERS (REALTIME-BASED, EQUATION-BASED, AND CELLULAR AUTOMATA-BASED) ..... 6
3.3 RISK MANAGEMENT STAGES ..... 6
3.3.1 IDENTIFICATION OF CRITICAL INFRASTRUCTURE ..... 7
3.3.2 ASSESSMENT AND ANALYSIS OF RISK ..... 7
3.3.3 MANAGEMENT IMPLEMENTATION OF RISK ..... 8
3.3.4 EFFECTIVENESS EVALUATION ..... 8
3.4 SOFTWARE SUPPORT ..... 8
3.5 OTHER RELEVANT CHARACTERISTICS IN CIP MODELLING APPROACHES ..... 8
3.5.1 DEPENDENCY AND INTERDEPENDENCY ..... 9
3.5.2 RESILIENCE ..... 10
3.5.3 POLICY AND REGULATIONS ..... 11
4. RESULTS AND ANALYSIS ..... 11
4.1 SOFTWARE SUPPORT ..... 12
4.2 SECTOR-BASED COMPARISON AND CLASSIFICATION ..... 12
4.3 MODELLING TECHNIQUES ..... 14
4.4 RISK MANAGEMENT STAGES ..... 15
4.5 SECTOR-BASED AND MODELLING TECHNIQUES ..... 16
4.6 RISK MANAGEMENT AND MODELLING TECHNIQUES ..... 17
4.7 RESILIENCE, DEPENDENCY AND POLICY AND REGULATIONS COVERAGE ..... 18
5 DISCUSSION OF FINDINGS AND CONCLUSIONS ..... 28
5.1 DISCUSSIONS ..... 28
5.1.1 – RQ1: WHAT ARE THE COMMON CIP APPROACHES (TOOLS AND TECHNIQUES) AVAILABLE FOR THE MANAGEMENT OF SECURITY RISK? ..... 28
5.1.2 – RQ2: WHICH ARE THE COMMON MODELLING TECHNIQUES APPLIED IN CIP APPROACHES? ..... 28
5.1.3 – RQ3: WHAT IS THE MOST APPLICATION MODE FOR EXISTING CIP APPROACHES? ..... 29
5.1.4 – RQ4: WHAT SECTORS ARE THE CIP APPROACHES CHIEFLY APPLIED? ..... 30

5.1.5 – RQ5: WHAT STAGES OF RISK MANAGEMENT ARE APTLY COVERED BY THE CIP APPROACHES? ..... 31
5.1.6 – RQ6: WHAT CIP APPROACHES CONSIDER RESILIENCE, (INTER)DEPENDENCY AND POLICY FORMULATION FACTORS, AND WHAT IS THE GENERAL CONSIDERATION LEVEL OF THESE THREE ATTRIBUTES IN REVIEWED CIP APPROACHES? ..... 31
5.2 SUMMARY AND RECOMMENDATIONS ..... 33
5.2.1 SUMMARY ..... 33
5.2.2 RECOMMENDATIONS ..... 36
5.3 CONCLUSION ..... 37
REFERENCES ..... 38
APPENDIX A: SUMMARY DESCRIPTION AND CHARACTERIZATION OF CRITICAL INFRASTRUCTURE APPROACHES (TOOLS AND TECHNIQUES) ..... 41

## List of Figures

Figure 1: Review Criteria for Critical Infrastructure Modelling and Protection Approaches ..... 4
Figure 2: Revised NIPP Critical Infrastructure Risk Management Framework [5] ..... 7
Figure 3: Cross Sector Critical Infrastructure Interdependency Representation, Source: (Simon, 2017) ..... 10
Figure 4: Software tool-based Support ..... 12
Figure 5: Sector-based Analysis of Occurrence of Critical Infrastructure Modelling and Protection Approaches ..... 13
Figure 6: Multi-Sector Application of Critical Infrastructure Modelling and Protection Approaches ..... 13
Figure 7: Modelling Techniques ..... 15
Figure 8: Risk Management Stages Covered ..... 16
Figure 9: Multi-Stage coverage of Risk Management Stages ..... 16
Figure 10: Sector-Based and Modelling Techniques Analysis ..... 17
Figure 11: Risk Stage and Modelling Techniques Analysis ..... 18
Figure 12: Analysis of Dependency, Resilience, and Policy Characteristics ..... 18

## List of Tables

Table 1: Criteria Meta-Data Analysis of CIP Approaches ..... 20

# Executive Summary

## Overview:

Critical infrastructures (CIs) – any asset with a functionality that is critical to normal societal functions, safety, security, economic or social well-being of people, and disruption or destruction of which would have a very significant negative societal impact. CIs are clearly central to the normal functioning of a nation's economy and require to be protected from both intentional and unintentional sabotages.

It is important to correctly discern and aptly manage security risks within CI domains. The protection (security) of CIs and their networks can provide clear benefits to owner organizations and nations including: enabling the attainment of a properly functioning social environment and economic market, improving service security, enabling integration to external markets, and enabling service recipients (consumers, clients, and users) to benefit from new and emerging technological developments. To effectively secure CI system, firstly, it is crucial to understand three things - what can happen, how likely it is to happen, and the consequences of such happenings.

One way to achieve this is through modelling and simulations of CI attributes, functionalities, operations, and behaviours to support security analysis perspectives, and especially considering the dynamics in trends and technological adoptions. Despite the availability of several security-related CI modelling approaches (tools and techniques), trends such as inter-networking, internet and IoT integrations raise new issues. Part of the issues relate to how to effectively (more precisely and realistically) model the complex behavior of interconnected CIs and their protection as system of systems (SoS).

This report attempts to address the broad goal around this issue by reviewing a sample of critical infrastructure protection approaches; comprising tools, techniques, and frameworks (methodologies). The analysis covers contexts relating to the types of critical infrastructures, applicable modelling techniques, risk management scope covered, considerations for resilience, interdependency, and policy and regulations factors.

## Key Findings:

This research presents the following key findings:

1. There is not a single specific Critical Infrastructure Protection (CIP) approach – tool, technique, methodology or framework – that exists or emerges as a 'fit-for-all'; to allow the modelling and simulation of cyber security risks, resilience, dependency, and impact attributes in all critical infrastructure set-ups.
2. Typically, two or more modelling techniques can be (need to be) merged to cover a broader scope and context of modelling and simulation applications (areas) to achieve desirable high-level protection and security for critical infrastructures.
3. Empirical-based, network-based, agent-based, and system dynamics-based modelling techniques are more widely used, and all offer gains for their use.
4. The deciding factors for choosing modelling techniques often rest on; complexity of use,

popularity of approach, types and objectives of user Organisation and sector.

5. The scope of modelling functions and operations also help to strike the balance between 'specificity' and 'generality' of modelling technique and approach for the gains of in-depth analysis and wider coverage respectively.
6. Interdependency and resilience modelling and simulations in critical infrastructure operations, as well as associated security and safety risks; are crucial characteristics that need to be considered and explored in revising existing or developing new CIP modelling approaches.

## Recommendations:

Key recommendations from this research include:

1. Other critical infrastructure sectors such as emergency services, food & agriculture, and dams; need to draw lessons from the energy and transportation sectors for the successive benefits of:
   i. Amplifying the drive and efforts towards evaluating and understanding security risks to their infrastructure and operations.
   ii. Support better understanding of any associated dependencies and cascading impacts.
   iii. Learning how to establish effective security and resilience.
   iv. Support the decision-making process linked with measuring the effectiveness of preparedness activities and investments.
   v. Improve the behavioural security-related responses of CI to disturbances or disruptions.

2. Security-related critical infrastructure modelling approaches should be developed or revised to include wider scopes of security risk management – from identification to effectiveness evaluations, to support:
   i. Appropriate alignment and responsiveness to the dynamic trends introduced by new technologies such as IoT and IIoT.
   ii. Dynamic security risk management – especially the assessment section needs to be more dynamic than static, to address the recurrent and impactful risks that emerge in critical infrastructures

# 1. Introduction

## 1.1 Background

A critical infrastructure (CI) is defined in the European Union Council Directive 2008/114/EC [1] as an asset, system or part thereof located in Member States which is critical for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a very substantial impact in a Member State as a result of the failure to maintain those functions. This definition positions CI as any functional system that supports standard workings of a nation's economy. Arguably, it has been described as a nation's economic "central nervous system" [2] – making it difficult for a nations with a properly functional or vulnerable CI to attain and sustain its missions and objectives of social and economic development and progress. There are increasing concerns and debates about the protection of CIs given the invaluable positions these have taken in social and economic developments.

Societal benefits are vastly reliant on the proper functioning of the various CI sectors [3]. More worrisome is the current trend where the drive for improved performance and efficiency in service delivery sees that CIs now hardly exist or function in isolation, rather they are typically tightly coupled into a system of (inter)dependent infrastructures [4], which now enable multiple and complex components and systems interconnectedness and interactions. Apart from the increased complexities, this trend of interconnectedness and infrastructure convergence also unveil a number of vulnerabilities and risks that threaten normal economic and social functionalities. Notwithstanding this, it is the integrated and reliable network of CIs that support and drive the actualization of a national and(or) international economic policy objectives and strategy.

As mentioned earlier, the benefits of CI can only be enjoyed if the infrastructures function properly. To function properly, CIs have to be safe from harm and secure from any significantly disruptive or damaging form of attack (cyber or physical) or compromise. Thus, it is imperative to ensure the protection of CIs, especially in the light of the growing and rapidly evolving maliciousness that target such infrastructures. It is important to know, and effectively manage security risks within CI domains. The protection of CIs and their networks can provide clear benefits to a nation including; enable the attainment of a properly functioning social environment and economic market, enhance the security of services, enable integration to and with external markets, and enable service recipients (consumers, clients, and users) to relish from new and emerging technological developments [2].

To effectively protect any system, it is necessary to first understand the security risks – learning about what can happen, how likely it is to happen, and the consequences of such happenings. Relative to CIs, effective protection then includes defining and managing security risks associated to CI elements and attributes. This include analysing vulnerabilities, assessing risks, implementing controls and mitigation procedures, and evaluating the effectiveness of adopted control/mitigation procedures [2]. Security threats relate to destructive or malicious actors and their actions against CI components, systems, or processes. Security vulnerabilities refers to flaws in the system which can be exploited to bring about harmful or undesired effects and failures in the system, affecting functionalities, operations, and system objectives.

## 1.2 Need for Comparative Survey

There is a growing recognition and acknowledgement that to effectively maintain and sustain operational continuity in critical infrastructures, resilience is a necessary protection objective

needed to compliment normal security capacities. Thus, emphasis is required on achieving resilience as much as it is underscored for security. Resilience ensure a capacity to adapt, withstand and recover swiftly from both intentional and unintentional attacks [5], [6]. Publications [7], [8] are available which emphasize the importance of understanding, modelling, and simulating CI attributes, functionalities, operations, and behaviours. These can help support security analysis perspectives, especially considering the dynamics in trends and technological adoptions. Although there are prior surveys and studies [9]–[12] on CIP modelling and simulation approaches, these works are not updated with newer approaches, and also do not address emerging phenomena such as resilience and government/organizational policy formation capabilities in modern CIs. The proliferation of interconnectedness and integration of internet-of-things (IoT) into CI setups raise new questions requiring answers about how to effectively (more precisely and realistically) model the complex behavior of interconnected CIs and their protection as system of systems (SoS). This question is yet open and calls for additional study.

This report presents an analyzed discourse of available CIP security tools, techniques, methodologies, and frameworks herein referred to as 'CIP approaches.' The covered approaches are studied and analyzed from a perspective of security risk management, and the extent covered by each CIP approach. The scope of approaches covered include: security analysis tools in software forms, descriptive methodologies and procedures, analytical or conceptual models that underscore any aspect of security risk modelling and simulation.

### 1.3 Research Questions

The aim of the report is to provide a concise review and analysis of CIP approaches. This is explored through highlighting the features that emphasize contexts around the strategic interests and trends associated with securing critical national infrastructures. By this we further seek to provide a usable reference that can aid critical infrastructure security developers, researchers, and users in the selection and adoption of appropriate security modelling and simulation approaches (tools, techniques and methodologies) suitable for their tailored environments and contexts (applications). In order to achieve the report's aim, the following research questions are explored:

1. *What are the common CIP Approaches (Tools and Techniques) available for the management of security risk?*
2. *Which are the common modelling techniques applied in the CIP approaches?*
3. *What is the most used application mode for existing CIP approaches?*
4. *What sectors are the CIP approaches chiefly applied?*
5. *What stages of risk management are aptly covered by the CIP approaches?*
6. *What CIP approaches consider resilience, (inter)dependency and policy formulation factors, and what is the general consideration level of these three attributes in reviewed CIP approaches?*

## 2. Methodology

In this section, we describe briefly how this study was conducted, including where and how relevant literature resources were obtained and examined to allow the identification of tools, techniques, or methodologies designed and applicable for the protection of CIs. The criteria used to analyze the CIP approaches are also described.

### 2.1 Literature Gathering

The study commenced with the gathering of relevant literatures from popular article databases. These include SCOPUS and Web of Science (WoS). Searches were also performed using the more

generic google search engine to gain pointer links to relevant published literatures that may have been omitted in the selected article databases. Search phrases used include: *'Critical Infrastructure Protection Tools'*, '*Critical Infrastructure Security Techniques', 'Critical Infrastructure Security Methodologies',* and *'Critical Infrastructure Security Management Methods'.* Using these search terms brought about the aggregation of related articles. However, to effectively address the above-listed research questions, contextual scopes and boundaries were adopted as criteria to guide the selection of most relevant literatures. These included:

- Research articles or reports on theoretical developments and(or) applications of security on CIs
- Review articles or reports on security modelling, analysis and(or) implementation techniques or tools with use case applications to any critical infrastructure sectors.
- Security risk assessment and management techniques/methods relative to critical infrastructures.

Based on these criteria, a total of 131 distinct CI protection modelling, simulation, and implementation approaches spanning software tools, techniques, methodologies, and frameworks were amassed from journal and conference articles, reports, and standards. These spanned from 1999 to 2017. These CIP approaches formed the sample of study and analysis from which the findings and conclusions of this were made.

## 3. Criteria for Comparative Evaluation of CIP Approaches

The critical infrastructure modelling and protection approaches contain procedural outlines and descriptions of techniques that can be used to collect and analyse information for CI protection purposes. Some of the procedures described have been extended into application-level programs/platforms to simplify and speed-up execution processes for CI protection/security. The programs appear as software designed to perform specific actions based on specific modelling techniques, e.g. collect or characterise component vulnerability information as part of the CI security risk management process. Thus, the reviewed CI tools and techniques are broadly classified based on four study contexts (as indicted in Figure 1), which include:

- Critical Infrastructure Types
- Modelling Technique
- Risk Management Stages
- Software Availability.

Criteria such as maturity and availability of CI tools were not used, although these have been used in the past [2] to evaluate CI tools. We think that there are uncertainties in accurately determining the maturity and availability status of some of the CIP tools given that they are mostly developed and used in-house. Reports and documentation on their use and effectiveness are scarcely available in public domain. Similarly, whether they have been discarded, modified or upgraded, and at what point; is an information not easily available in the public domain. We think that adopting such criteria with potential for inaccurate data can greatly affect the accuracy of the overall study.

### 3.1 Sectors of Critical Infrastructure (CI)

The list of Critical Infrastructures (CI) sectors covered in this review involved a compilation of sector outlines from the Revised US National Infrastructure Protection Plan: NIPP [5], the European Union Directive 114/08 [1] and the UK CPNI documentation [13].

From this literature, a harmonised list of critical infrastructure sectors that this study focuses on, emphasising the need for security risk prevention and protection. The list includes: Energy (electricity, oil, natural gas), Chemical, Industrial Control, Dams, Defense Industries, Emergency

Services, Financial Services, Food and Agriculture, Government facilities, Commercial Services, Health and Public Health, Transportation, (Railways, Roads, Highways, Aviation, Shipping and Ports), Water and Waste water, Information Technology and Telecommunication, Nuclear.

While in the study, we draw particular attention to CI modelling and protection approaches and analysis outcomes that relate or apply to critical national infrastructures (CNI) sectors. The UK CPNI definition of critical national infrastructures refers to those CI facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the United Kingdom depends and which ensure the country continues to function socially and economically [14]. Out of the 15 critical infrastructure areas listed, 9 have been categorised as CNI by UK's CPNI. These include: Communications, Emergency Services, Energy, Financial Services, Food, Government, Health, Transport, and Water [14], [15]. These are considered 'nationally critical' because of the impact they contribute to the normal functioning of the national economy. For example, communications sector is listed first because of its unrivalled value. The improper functioning of the communications sector in modern times can lead to a crippling of other critical infrastructure sectors equally important – causing very significant threat to the national economy, social order, and by extension, political order [15].

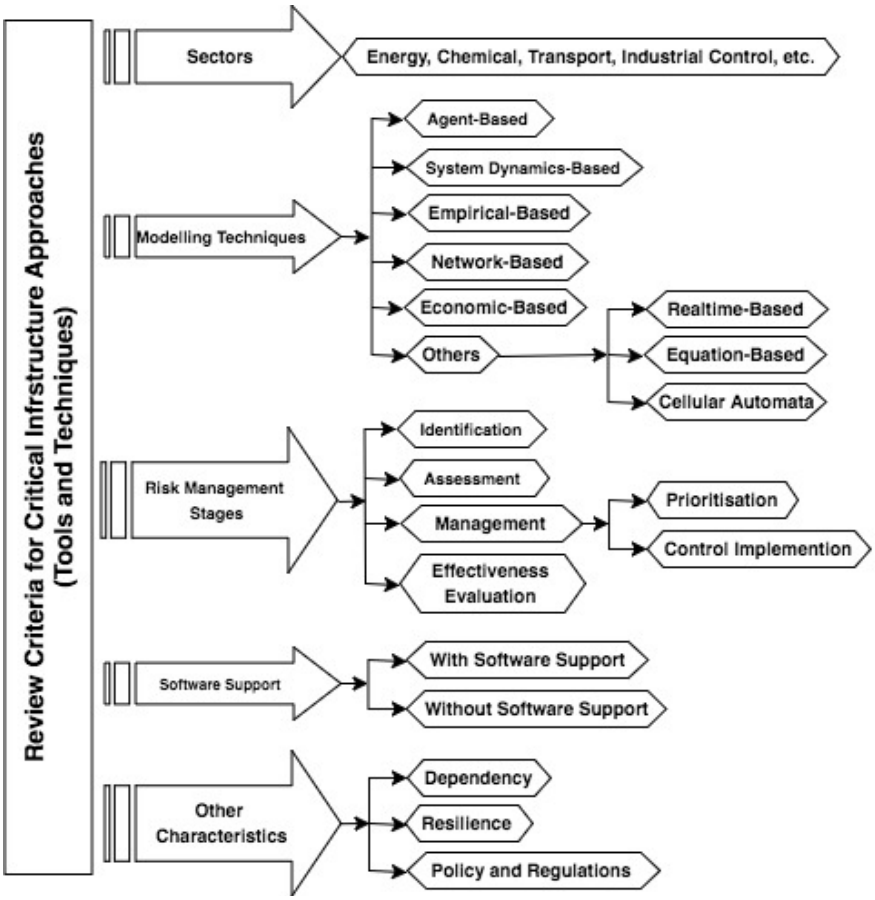


*Figure 1: Review Criteria for Critical Infrastructure Modelling and Protection Approaches*

### 3.2 Modelling Techniques for CIs

CNI modelling techniques refer to methodologies applied to critical infrastructure protection. These methodologies and techniques follow different simulation paradigms and decision-making processes that are often dependent on the desired purpose of each tool. A common goal of all the techniques is the attainment of risk assessment, though at varied contexts and extents. We use the

classifications proposed by Ouyang [16] as the bases for our review of CNI tools and techniques. The researcher noted that CNI protection tools may be characterised into six modelling and simulation approaches. These include: Agent-based, system dynamics, empirical, network, economic, and other (equation-based, real-time simulation, and cellular automata) techniques. These modelling techniques are often combined with additional computational methods such as discrete time-step, continuous time-step, Monte Carlo, decision-trees, geographical information systems, event monitoring, risk management, etc. [2].

### 3.2.1 Agent-based

Agent-based modelling is a technique for modelling systems as a collection of autonomous decision-making entities referred to as agents [17]. In agent-based approach where individual entities and their interaction with each other and their environment are clearly represented in a program. CIs are typically viewed as complex adaptive systems (CAS) due to the complexity of the interrelationships and interaction, and the associated decision-making processes involved. Agent-based approaches are used to model CIs as CAS using a bottom-up approach that assumes that complex behaviour or scenario surfaces from several individual and relatively simple interactions of autonomous CI components as agents [18], [19]. Agent-based approach provides a more common technique for developing modelling and simulation tools.

### 3.2.2 System Dynamics-based

System dynamics modelling is a technique for studying and managing complex feedback systems. A top-down approach is adopted for analysing complex adaptive systems involving interdependencies [20], [21]. System dynamics is typically characterised by feedbacks, stocks and flows. Feedback loops suggest linkage and direction of effects between CI components, and stocks represent quantities or system states whose levels are controlled over time by flow rates between stocks. System dynamics approaches can be used for interdependency modelling using the causal-loop and stock-and-flow diagrams [19], [20].

### 3.2.3 Empirical-based

Empirical modelling is a technique for analysing CI interdependencies from historical occurrences and data from destructive incidents, and knowledge/experience from experts [16], [22]. This approach is particularly useful when parametric models of a system under study cannot be developed. Studying and analysing system (CIs) interdependencies using empirical approaches such as those in [23]–[27] can support the identification of frequent and critical patterns of failure in CI. Interdependency strength metrics can be quantified to guide decision-making. The approach can also support experiment-based analysis of risks in interdependent CI and provide alternatives for the minimisation of risks.

### 3.2.4 Network-based

Network-based modelling technique refers to the approach for modelling CIs in the form of networks where nodes symbolise different CI components, and links that simulate the physical and relational connections amongst the components [16], [28]. In the network-based approach, CIs are modelled to capture and demonstrate interdependencies, and provide intuitive representations of the CIs along with clear and thorough descriptions of the network topologies and the patterns of flow. The failure of components due to inherent hazards can easily be modelled and analysed to determine performance response on the CI [29]–[31]. Cascading failures within and across CIs can also be simulated and analysed from a system-level perspective [32].

### 3.2.5 Economics-based

Economics-based modelling techniques involve analysing CI interdependencies through perspectives of economic cross-reliance [33]. The economic model approach can follow an input-output or computable general equilibrium theory concepts. The input-output theory provides a more common approach where the risk of inoperability is evaluated; viewed as and from the inability of a CI to accomplish its intended functions. Thus, inoperability concept can be used to analyse how perturbation propagate through interconnected CIs and how effective mitigations can be achieved [34], [35]. Interdependencies among infrastructure sectors are evaluated using economic relationships.

### 3.2.6 Others (Realtime-based, Equation-based, and Cellular automata-based)

Besides the modelling approaches presented above, couple of other modelling techniques and approaches exist which does apply to critical infrastructures and can be used to analyse interdependencies. These include: (i) Real-Time Simulation-based techniques, where real-time quantitative measurements of CI system states are obtained to gain situational insights. This is can support time-critical decision-making. This approach is used to study and represent CI systems, where interdependencies mean that failures in one infrastructure rapids affects the states of other valuable infrastructures linked to the affected infrastructure [36]. (ii) Cellular-automata techniques, where phenomena especially related to understanding future states are modelled using microscopic cellular automata theories of change. An example use case is the simulation/evaluation of system performance of mass transit with respect to future passenger demand [37]. Finally, (iii) Equation-based techniques involving the use of mathematical models to capture and represent the varied attributes and characteristics of a CI [16]. An example is the use of hierarchical holographic modelling [38], [39] which uses multiple maths models to capture multiple dimensions and perspectives of CIs.

In this review, the above modelling classifications as presented by Ouyang [16] are used to categorise and analyse aggregated CNI security tools, techniques and methodologies. To effectively map all the CNI tools and methodologies obtained, each is assigned to a relative or appropriate category that fits its formation or functional characteristics. We note that some of the tools demonstrate characteristics spanning multiple modelling techniques. In this case, the mapping of an affected CNI tool or methodology is related to the specific modelling techniques affected. This way, techniques that leverage multi-modelling capabilities are distinguished from others.

## 3.3 Risk Management Stages

There is some agreement that risk management approach provides an effective solution towards achieving security for industrial controls and critical national infrastructures [9], [40]. From literature [41], [42], risk assessment and management approaches vary in one or both of two ways: (i) the nature of approach, and (ii) how risk is measured. Based on this work's focus on critical infrastructures, the former approach to viewing risk is adopted – noting the emphasis around critical assets, the potential harm that can be done to them, and the rippling effects that can affect other connected assets on the criticality chain. Thus, this study is conducted based on an analysis of risk management stages supported or incorporated into aggregated CI tools and techniques. This way, the purpose served by of each tool or technique is underscored. This is done based on the NIPP (National Infrastructure Protection Plan) Critical Infrastructure Risk Management framework [5]. According to the NIPP Risk framework, tools, techniques, and methodologies for CNI protection can be classified according to the purpose they serve. The purposes are demonstrated by the stage(s) of the overall CI risk management framework that is(are) supported in their application processes

and associated outputs. A model of the updated framework for CI security and resilience is presented in Figure 2.

From figure 2, CI elements can take one of three dimensions: physical, cyber and human. The model also included a process of recurrent information sharing and feedback into subsequent stages of risk management. Aside from the initial stage of setting security goals and objectives, other key stages of the framework include: identification of infrastructure assets, assessment and analysis of risks, risk management implementation (prioritisation and Control), and measurement of effectiveness. However, to achieve clearer outcomes, we performed initial analysis of the CI tools and methodologies with a decomposed form of the stages of the NIPP framework. Here, the risk management implementation stage was further split into its sub-stages: (i) risk prioritisation and (ii) risk control. This allows us to better characterise the scope of risk management to which each tool or methodology serves from a purpose point of view.

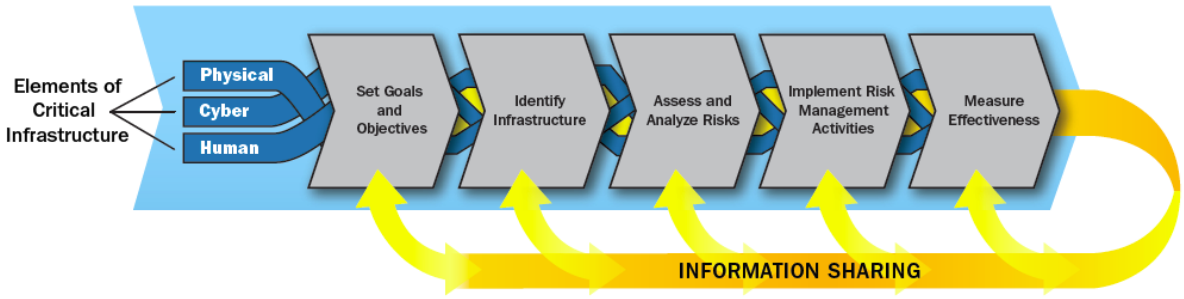


*Figure 2: Revised NIPP Critical Infrastructure Risk Management Framework* [5]

### 3.3.1 Identification of Critical Infrastructure

This involves the identification of assets including CI components, networks, systems, functions, and the resources encompassed (including human attributes) and associated information that are directly crucial and critical to continued operations. It also includes identifying potential vulnerabilities and associated (inter)dependencies which exploitation can bring about critical impacts. Critical infrastructures (components, systems, and networks) listed through this process comprise those which, if damaged or unsettled, could trigger some combination of substantial economic losses, or widespread and lasting impacts to national comfort and governance capacity [5], [12]. Thus, this process can include identifying indirectly linked infrastructures that are critical to the functioning of a primary CI and might be picked up by attackers as potential vectors of attack. Considering this from the aspect of infrastructure dependencies and indirect criticality can help support a more effective CI protection. For example, a nation's Water and Wastewater control system infrastructures often depend on energy (power) infrastructures to function. Identifying the critical power supply assets linked to the Water or Wastewater control infrastructures is also crucial towards obtaining a broader perspective of critical infrastructure security risk. Thus, this process requires a complete inventory of the CI setup along with interdependent systems. The pursuit of resilience starts from understanding these perspectives and information about the system of interest.

### 3.3.2 Assessment and Analysis of Risk

This stage involves evaluating security risk associated to the assets identified and their related functions. It includes understanding the security threats to the CI assets, the potential vulnerabilities and events within the system context and their inter-relationships, and estimating the consequences and(or) impacts (many of which have been defined in research [43]) if identified threats exploit identified vulnerabilities within the system. The assessment of risk event likelihoods

and consequences may be explored from cost, schedule, performance, or functionality points of view, and can take quantitative or qualitative dimensions [5]. Typically, the process is quite systematic and laborious considering both system and component-level interactions and interdependencies.

### 3.3.3 Management Implementation of Risk

After assessing risks, it is typical to act upon risk derivations to bring about effective controls. However, decision-makers require strong basis for actions, hence the desire to prioritize activities sets-in to manage CIs risks based on associated criticality of the affected infrastructure, the cost of associated activity, or the risk control or reduction. Thus, the activities of managing security risk can be broken down into two: risk prioritization analysis, and risk mitigation planning/implementation.

*i. Risk Prioritization Analysis*

This stage involves combining and analyzing evaluated risk results in order to identify where security risk mitigation may be more compelling to inform easy appropriation of protective measures. It involves comparing risk levels and resource sectors and establishing priorities to support assessing risk criticalities using decision-analytics rules to rank risks for the most to the least critical. This way, a more cost-effective and productive security decision can be achieved.

*ii. Risk Mitigation Planning and Implementation*

This stage is aimed at reducing security risks through deploying or engaging specific protective (security) measures. Guided by the outputs of prioritization, sector-appropriate security measures, actions or programs are chosen and implemented to reduce or manage identified risks.

### 3.3.4 Effectiveness Evaluation

This stage involves evaluating how effective selected and implemented security measures and strategies have been. This is established from a system of descriptive and process-based indicators that provide evidence on how and the extent to which desired security goals are achieved. Where necessary, existing and newly identified risk events are also reevaluated. The CI tools and methodologies are analysed and classified according to the CI security and resilience risk purpose served and stages of risk management methodology covered.

## 3.4 Software Support

The tools and methodologies were also classified according to their level of development and application demonstrated either as procedural descriptions (workflows) of methods or as software products to achieve the purpose intended. This allows for understanding the trends in modelling and security analysis to support adoption and use by interested parties.

## 3.5 Other Relevant Characteristics in CIP Modelling Approaches

Typically, most critical infrastructures are characterized by a myriad of complexities most notably in connections and interactions. Now the trend of interconnecting CIs via geographically-distributed networks and physical hardware-based channels [44] has enabled dependencies and interdependencies amongst linked infrastructures. This means that a disruption or failure due to natural or human-initiated events can spread consequences to other CIs not directly targeted but linked to a target. This is considered a cascading effect [45] which negatively imparts on a wider aspect of the network of CIs and by extension the society [46]. The harmful impacts can be physical or digital, economic, psychological, reputational, social and societal [43]. To considerably manage the grave consequences of interdependencies amongst CIs, a resilience capacity provides a good

solution approach by ensuring that functionalities and operations are reasonably maintained even in the face of an infrastructure compromise or hack [47]. This can be better achieved following proper guidelines, hence the need for effective security-related policies and regulations. This discourse also underscores the extent to which the relevant characteristics - *dependency, resilience*, and *policy and regulations*; are leveraged or reflected in the reviewed CIP approaches.

### 3.5.1 Dependency and Interdependency

As technology continues to evolve, and more interests and actions incline towards convergence and interconnectedness of multiple CIs to improve operations and services, cascading impacts due to direct and indirect infrastructure dependencies and interdependencies are as probable as the actual cyber-attacks or compromises of CIs themselves. A growing body of research is seen around quantitatively modelling complex CI systems with stern focus and interest on underscoring system dependencies and their associated implications, and the use of such information to understand the scales of impact cascades [48]–[50]. These works emphasis the clear lesson that; the understanding of CI as a 'system of systems' (functionalities and complexities) can be significantly improved by identifying and characterizing dependencies associated to every CI. This has to be relative to system or component failures and disruptions, and the corresponding impacts on other connected CIs. The complexity of connections and interactions amongst CI components may pose some challenge towards effectively achieving this, however, such understanding (when gained) can support the design of effective controls and response strategies [51]. Thus, dependency within and amongst CI is quite crucial for achieving or undermining acceptable system security, safety and dependability [52]. Indeed, the need to understand dependencies is motivated by the several catastrophic cascades in CI disruptions [47], [53], [54] which are direct consequences of dependencies inherent.

CIs protection (CIP) tools, techniques, methodologies, models and simulations can provide ways of understanding CI systems, their interdependencies, their vulnerabilities, the consequences and impacts of disruptions and failures, and the associated cascades through and across connected CI components and systems. These can be achieved from a risk management dimensions related to CI involved [12]. Other researches [2], [9], [55] also share similar view alluding to risk management to provide a more effective approach for underscoring and responding to cyber security issues in CI contexts. According to [2], most critical infrastructure protection efforts, plans, and implementations are typically based on risk management frameworks conceived as national or global standards. Figure 3 presents an illustration of some critical infrastructure sectors dependencies. The arrows are used to depict the direction of dependency for an originating sector with the associated description of the nature of dependency involved. For example, an arrow moving from the electric power sector to the transportation indicates a dependency where the transportation depended on the supply of power for its signaling switches. Similarly, the natural gas sector depends on the transport for shipping its products.

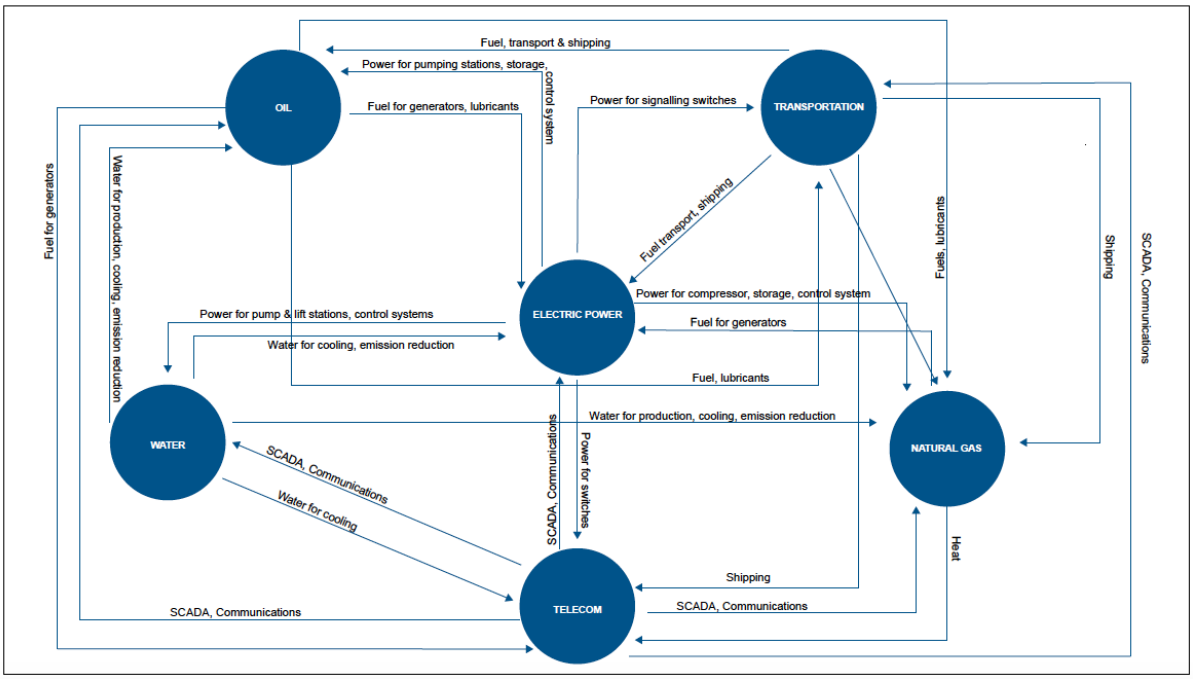


*Figure 3: Cross Sector Critical Infrastructure Interdependency Representation, Source:* [56]

### 3.5.2 Resilience

With the impacts of critical infrastructure cyber-attacks and disruptions potentially grave due to the dependency phenomenon described, the need to ensure that the critical infrastructure sector operators and the society in general are well-found and equipped to withstand and recuperate from such adverse events is ever more necessary now. Most times the events happen unexpected, and complete control is rarely feasible, thus, ensuring the appropriate readiness and recovery, requires channelling efforts into reducing the vulnerabilities of CI components and systems which support the economic, environmental and security activities of modern societies. In line with this, the emphasis is on developing and adopting CI resilience concepts that integrate approaches to planning, response, and recovery from incidents effects. Resilience is defined as *"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."* [5].

The main argument for resilience is that due to the adverse and changing landscape of hazards and threats to CI, it is not possible to foresee, prevent, prepare for or mitigate all of these events, which in several cases can be unknown or emergent [47]. Protective security measures alone cannot mitigate supply chain disruption, nor ensure the rapid restoration of services. Owners and operators of critical infrastructure often have limited capacity to continue operations indefinitely if the essential goods and services they require are interrupted [57]. Quite supportively, resilience is now being viewed as fundamental in general crisis and disaster management discourse, and is the focus of widespread efforts for resisting, absorbing, accommodating and recovering from the effects of security threats. Resilience emphases preventive, mitigative and preparedness activities prior to the crisis, and the response during the crisis. Most notably, it also deals with recovery after the crisis, in the event of the disruption of a CI service, for example [6]. Thus, CI resilience emphasizes more on the whole cycle of a crisis, since it is impracticable to guard against all threats. However, in addressing CI resilience, it is also very crucial to consider the integral dependencies that exist among most of the modern CI, as well as the cascading failures and impacts through multiple CIs [57], [58].

### 3.5.3 Policy and Regulations

Another key feature that was considered is *'Policy and Regulations'*. Some of the CIP approaches are products of national critical infrastructure plans where government institutions are involved in defining security strategies and initiatives necessary to help achieve the protection of the national critical infrastructures from both natural and man-made threats and disasters. Thus, some of the security approaches clearly emphasised the importance of policies and regulations and their inclusion as objectives in CI approaches.

In general, the formulation of CIP policies and regulations can support effective decision-making. Examples of these plans include: UK Initiative for Critical Infrastructure sectors [13] with the purpose of developing policies for the protections of critical infrastructure sectors, their resources and services. Australian National Strategy for Critical Infrastructure Protection [57] with a driving objective of enabling a capability to undertake national defence and homeland security. Canadian Strategy for the Protection of National Critical Infrastructure [59] with the purpose of exploring security capacities for physical ad cyber components to be applied in both public and private sectors. As a result, several security risk management techniques and tools have been developed and adopted by various CI sectors to address their security threats and the potential consequences. Although all of these tools, techniques, methodologies and frameworks share a common goal of seeking to assure or enhance security and by extension safety within their associated CI domains, there are differences in the scopes, approaches, and extents to which the prescribed goals of security and safety are being pursued by the different tools, techniques, methodologies, and frameworks. For easy understanding, we use the term 'approaches' as a general term to refer to the CIP tools, techniques, methodologies, and frameworks reviewed in this study.

## 4. Results and Analysis

The security of critical national infrastructures (CNI) typically follow risk management approaches and frameworks, but often a varied levels and coverages. The NIPP framework seem to provide the most commonly supported guidelines in security objectives, strategies, and sector coverage. It also provides references points to a wider community of nations and infrastructure sectors exploring the development of tailored infrastructure security methodologies, tools and techniques [5]. The tools and methodologies reviewed in this report have not been directly applied by our own work, but information about their applications, features and functionalities were gathered from bibliographic literatures: reports, articles, and standards to arrive at informed insights. The list of CIP security tools and techniques represented in this report is not quite exhaustive, however, it does reflect most of the research being conducted in the area of critical infrastructure protection and considered relevant in the light of the considerations for incorporating IoT into existing systems.

The Table 1 presents a summarised outline and criteria-based evaluation of the CIP tools and techniques classification, the results of the review are also presented. A total of 131 CIP approaches formed the initial set of results found. The findings of the report only represent views derived from the data analysed from the review and does not reflect any external information. Where originally available from source documents, the acronym for each CIP approach is used, and where acronyms are not available from the source document, we formed acronyms using keywords found in the descriptive titles of the affected CIP approaches. This was done to simplify referencing to each approach in the analysis and discussion stages of the report.

### 4.1 Software Support

As indicated in Figure 4, 70 (nearly 53%) of the CIP approaches indicate provision or representation as customised web-based or standalone software tools, or mention that another form of modelling software e.g. MatLab can be used to demonstrate the approach. 62 (about 47%) are not directly represented as software nor do they mention any affiliation to existing simulation software. These approaches principally exist as methodologies which define procedures and techniques that define or describe how protection (security) can be implemented or achieved. Essentially methodologies comprise theoretical/conceptual process or activity-flows descriptions for characterising security risks in CI environments.

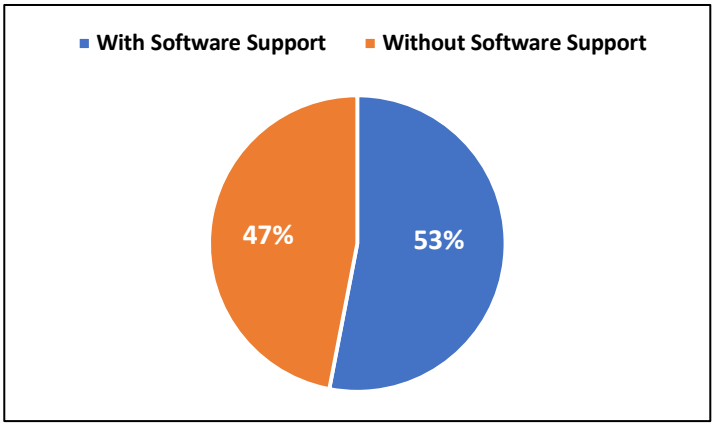


*Figure 4: Software tool-based Support*

### 4.2 Sector-based Comparison and Classification

Categorising the CIP tools and techniques based on their sectors of application provides insights into the CI areas where wider interest and effort for security modelling and analysis are focused. We note that some tools have applications to multiple sectors. Typically, multiple applications meant that such tools could be used independently in the applicable sectors, hence, for the evaluation, each application of a tool to a specific sector was evaluated independently. This implies a multi-counting for tools with applications to multiple sectors. This can help reveal CI sectors with less efforts and where attention may be required. The results in Figure 5 indicate that more than half (72, representing 54.5%) bear applications to the energy critical infrastructures, which spans electricity, pipeline & oil, natural gas sectors. The transportation sector CI also enjoy significant application support by 42 tools (37.1%). These are closely followed by the critical infrastructure sectors for Water & Waste Water (47, representing 35.6%), Chemical (41, representing 31.1%), and Commercial Facilities (40, representing 30.3%) of the total CIP tools and techniques covered in this study. Emergency Services which is also considered a CNI has the least (13 – representing 9.8%) number of applicable CIP tools and techniques.

From Figure 5, it can be observed that of the top 10 CI sectors with the highest number of tool/methodology applications, 6 sectors (Information technology & Telecommunications, Energy, Financial Services, Health & Public Health, Transportation, Water & Waste Water) are listed as critical national infrastructures by the UK CPNI [14]. Besides emergency services, other CNI sectors that do not have as much attention in terms of security modelling and analysis include: food & agriculture (12.1%) and government facilities (20.5%). Nearly 17.5% (23) of the reviewed CIP techniques relate to the activities of human agents with respect to checks, verifications and responses to critical infrastructures especially in cases of emergencies and policy recommendations related to security and safety. As will be discussed later, policy regulation and implementation (PRI) are quite relevant in critical infrastructure security. As observed in the methodologies such as Athena, N-ABLE, CIP/DSS, HAZOP, and Risk Maps, etc., which consider PRI feature, it is typically

accomplished through evaluating the successes from potential recommendations and the corresponding decisions taken to ensure security and safety resilience and prevent emergencies.

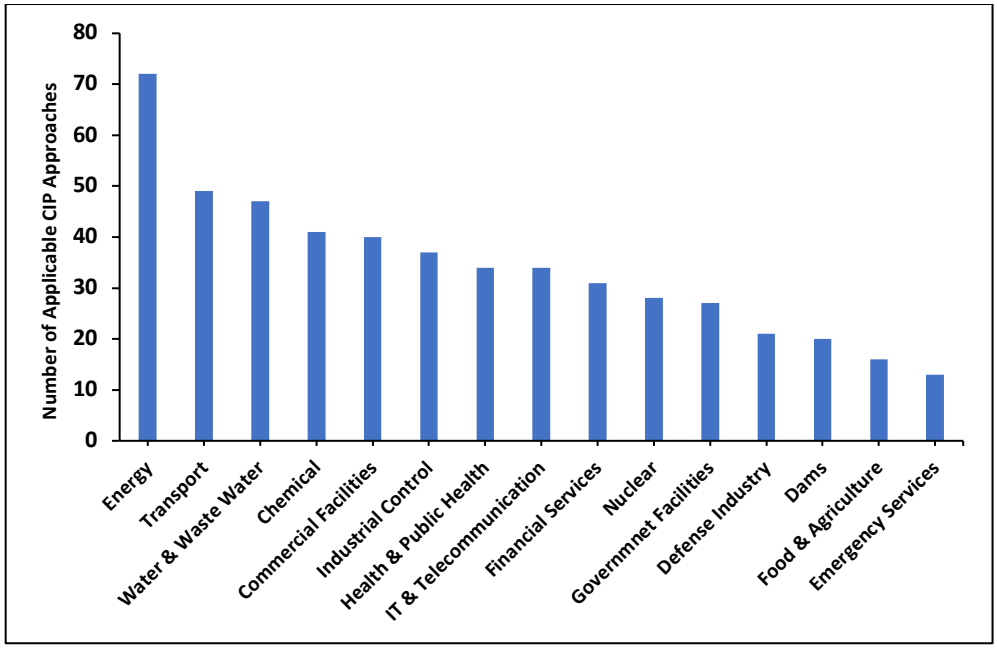


*Figure 5: Sector-based Analysis of Occurrence of Critical Infrastructure Modelling and Protection Approaches*

From a multi-sector application perspective, Figure 6 indicates most (111 – representing 84.1%) of the CIP approaches mainly cover up to 5 sectors (1-5 sectors). 60 out of the 111 provide software support for engaging and implementing their designed operational processes. 4 (3%) of the CIP approaches mainly cover between 6 to 10 sectors. These include: IIM, Risk Map, RVA, and BLDMP. Only 1 (IIM) provides software support. 16 (12.1%) of the CIP approaches (Athena, BIRR, CASCADE, CIDA, CIMSuite, CIP/DSS, CIPDSS-DM, EURACOM, Fort Future, IRRIS, NIPP-RMF, HM-BRMCI, ACT, Cy-T SCADA-RF, CORAS-BRA-SCADA, and ICS-CDTP) cover at least 11 CI sectors, and 9 of the approaches provide software support.

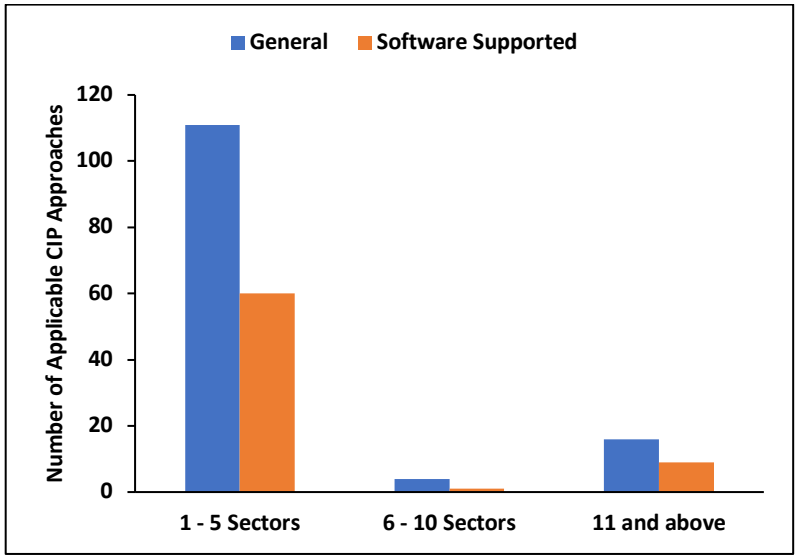


*Figure 6: Multi-Sector Application of Critical Infrastructure Modelling and Protection Approaches*

### 4.3 Modelling Techniques

Based on modelling techniques, a wide acknowledgement and adoption of simulation schemes is observed. Results in Figure 7 indicate that Agent-based modelling approach is adopted by 26 (about 19.7%) of reviewed approaches. Example of approaches under this modelling class include: ActivitySim, AIMS, CIMS, CISIA, ADVISE, N-ABLE, GoRAF, FINSIM, COMM-ASPEN, and NG Analysis Tools. System dynamics-based modelling is adopted by 20 (about 15.2%) of the reviewed approaches, examples here include: AIMSUN, CIMSuite, CIPMA, I2SIM, Modular Dynamic Model, RA-SCADA Railways, ACT, BLDMP, QTRIM, and ICS-CDTP. 32 (24.2%) approaches leverage network-based modelling approach. Examples of tools in this group include: CASCADE, CIDA, IRRIIS, MBRA, NEMO, MUNICIPAL, R-NAS, TRAGIS, HAZOP, LUND, TIMQAV-CIS, CSRA-NPP, and PMU-Based RAFPCS. Also, there appear to be a higher number (36, i.e., 27.3%) of tools and methodologies leveraging empirical-based modelling approach. Example of approaches in this class include: HURT, LogiSims, Restore, TEVA, EAR-PILAR, FTA, MIA, RVA, RMCIS, SAIV, VINCI, ATAV-SCADA, and CORAS-BRA-SCADA. The complete list of reviewed CIP approaches and their associated modelling techniques are presented in Table 1.

Other modelling approaches which have enjoyed moderate acceptance and use include: cellular automata-based modelling – 2 (1.5%) approaches (EPRAM and NSRM), economic-based modelling – 5 (3.8%) approaches (CEEESA, ACT, IRAM-SCADA Info Sec, and QCSRAM-SCADA), equation-based modelling – 7 (5.3%) approaches (PC Tides, RADR, VACSPI, RAMCA, SC-Based ARAC, IRAM-SCADA Infor. Sec, and QMACSR-SCADA Systems), and real-time simulation approaches - 12 (9.1%) approaches (RTDS, DUTCH NRA, ECI-GIS, GAMS-CERO-ERA, GoRAF, UML-CI, Sandia Risk Assessment, RAIM, TIMQAV-CIS, ADVISE, CORAS-BRA-SCADA, and PMU-Based RAFPCS). 5 (3.8%) approaches do not have any modelling approach but constitute descriptive workflow methodologies for CIP modelling and analysis. These include: BIRR, COUNTERACT, DECRIS, EURACOM, and UPMoST.

It is also noted that some of the CIP approaches combine two or more modelling techniques in a security analysis process. Some of the approaches in this group include: IRAM-SCADA-Info-Sec approach which combines economy-based and equation-based modelling techniques. ACT combines economy-based and system dynamics-based modelling. PMU-Based RAFPCS and TIMQAV-CIS approaches both combine network-based and real-time simulation techniques. CORAS-BRA-SCADA combines empirical-based and real-time simulation techniques. ADVISE and GoRAF approaches combine agent-based and real-time simulation techniques.

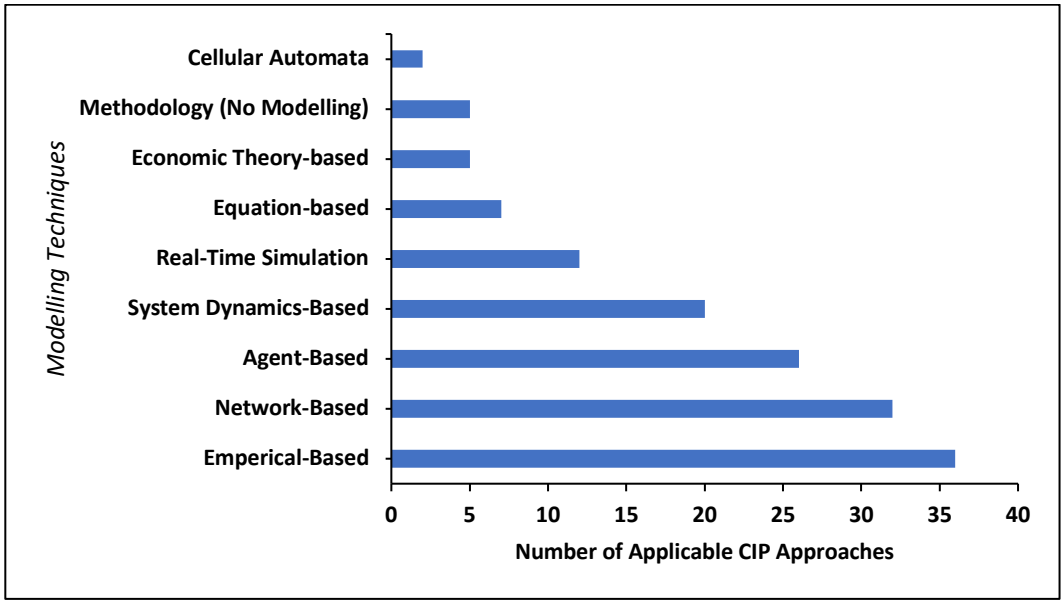


*Figure 7: Modelling Techniques*

### 4.4 Risk Management Stages

Based on the risk management methodology presented in Figure 8, the reviewed CIP tools and techniques can be categorised according to the risk management stages they cover. From this, useful insights can be drawn. 98 (representing 74%) CIP tools and techniques included/covered aspects related to identification of critical infrastructures and vulnerabilities, and 91 (68%) CIP tools and techniques covered assessment of risks. A total of 82 CIP tools and techniques covered some sort of risk management implementation - a stage consisting and combining risk prioritisation and risk control sub-stages based on the revised NIPP Critical Infrastructure Risk Management framework [5] in Figure 2. From these, 20 (nearly 24%) tools covered risk prioritisation stage alone without control implementations, while 29 (nearly 35%) tools and techniques covered risk control implementation stage alone without any form of prioritisation. For the effectiveness evaluation, 34 (nearly 26%) CIP tools and techniques captured this stage of the revised risk management framework.

Looking at the risk management implementation sub-stages (prioritisation and control) in isolation, more (58 – nearly 44% of 131) CIP tools covered some sort of risk control implementation than risk prioritisation which had 49 CIP tools. The 58 tools also represent 54% of the CIP tools and techniques categorised under the risk management implementation stage. Half (29) of the tools covered both risk prioritisation and control implementation stages, the remaining half covered just one of the two stages.

It is observed from results that not much of the existing tools and techniques are able to cover all the stages individually. From Figure 9, it is shown that 65 (nearly 49%) of the CIP tools and techniques cover only two stages, which most typically include: risk identification and risk assessment. 56 (nearly 42%) of the CIP tools and techniques cover between 3 - 4 stages. Only 6 (nearly 4.5%) of the CIP tools and techniques covered all five stages. These include: BIRR, COUNTERACT, EURACOM, IRRIIS, NSRAM, and NIPP-RMF itself. We observe that these tools exist as either broad guiding frameworks such as NIPP-RMF, mostly methodologies (BIRR, COUNTERACT, EURACOM, IRRIIS), or complex modelling tool (NSRAM) with software support. The methodologies and framework are mostly applicable to a generality of the critical infrastructure sectors, while the

software modelling tool NSRAM is typically applicable for chemical, energy and IT/Communications infrastructure sectors.

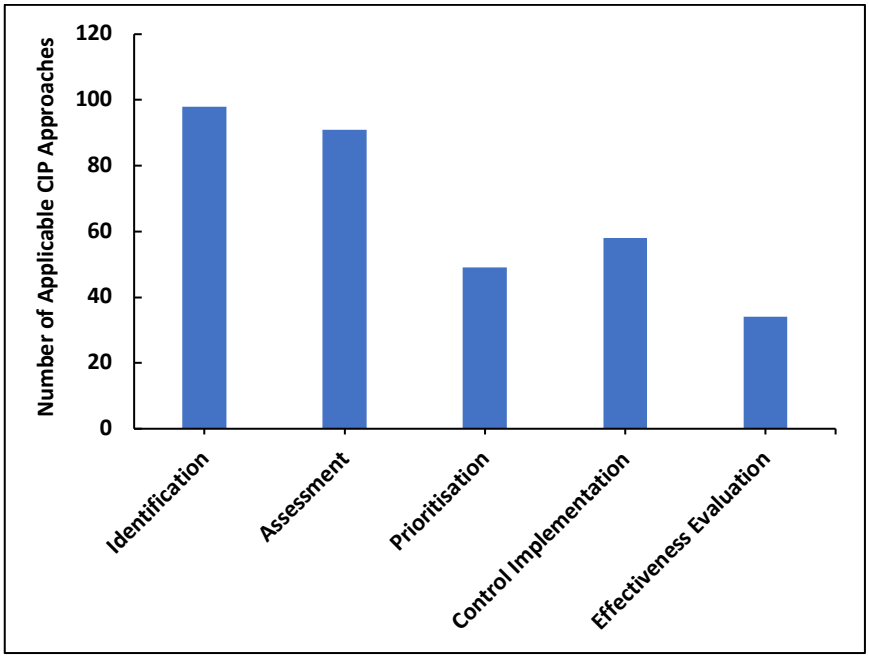


*Figure 8: Risk Management Stages Covered*

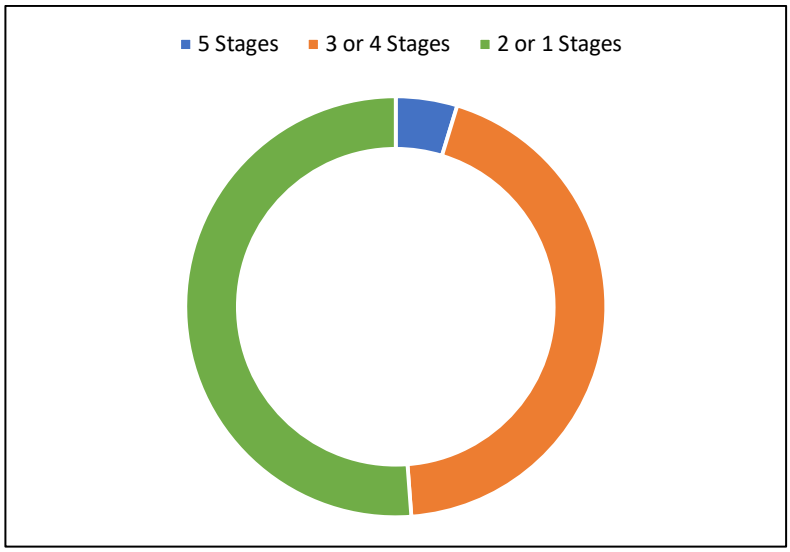


*Figure 9: Multi-Stage coverage of Risk Management Stages*

### 4.5 Sector-Based and Modelling Techniques

As shown in Table 1, CIP tools and techniques in this survey can be categorised based on the infrastructure sector areas where they can apply. They are also represented using various modelling approaches (tools and techniques). The results of a cross-criteria analysis involving modelling and simulation techniques (relative to the surveyed tools and techniques) employed in each of the critical infrastructure sectors covered is presented in Figure 10.

With the widest attention on the energy infrastructure sector covering: electricity, pipeline & oil, and natural gas, network-based modelling appears to be most widely adopted with 21 CIP tools and

techniques. This is closely followed by the empirical (18 tools) and agent-based (14 tools) simulation methods respectively. Other critical infrastructure sectors where network-based modelling technique is chiefly adopted include: Transport (18 tools), Water and Waste Water (11), Nuclear (11), and Chemical (10). However, for the empirical modelling technique, the more common applicable sectors appear to vary from those of network-based. The sectors where empirical-based modelling and simulation appear to be more used include: Industrial Control (16 tools), IT & Telecommunications (13 tools), and Government facilities (13 tools).

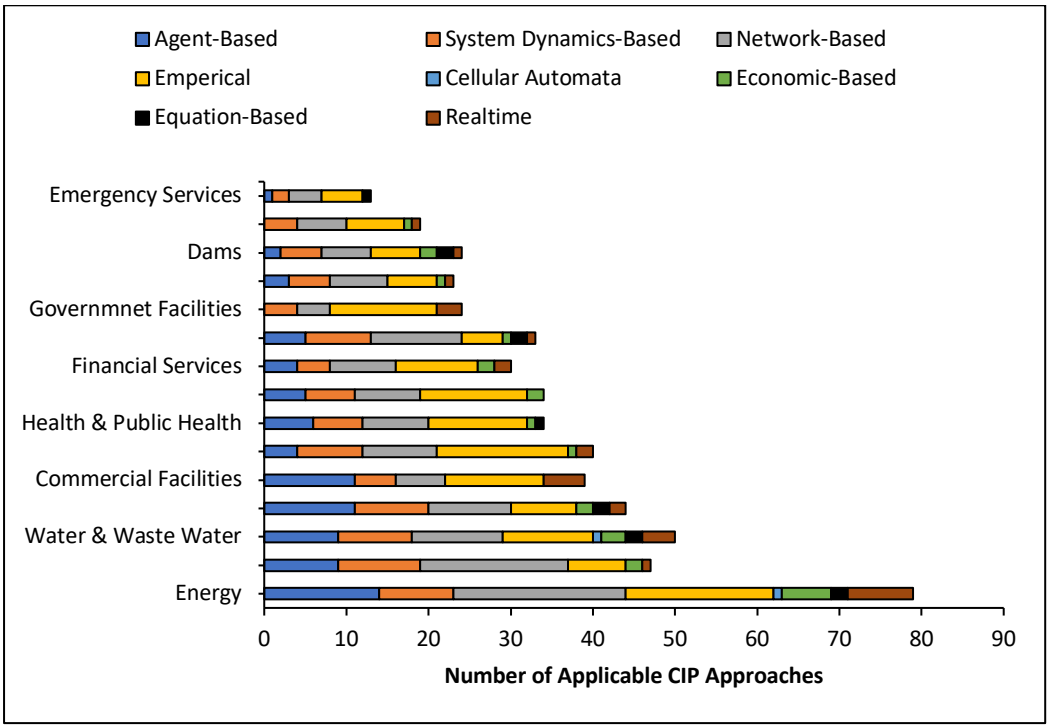


*Figure 10: Sector-Based and Modelling Techniques Analysis*

### 4.6 Risk Management and Modelling Techniques

Analysing the reviewed CIP tools and techniques in relation to the applicable security risk management sub-stages, it is observed from Figure 11 that empirical-based modelling (applied in 27 CIP approaches), network-based modelling (applied in 26 CIP approaches) are more widely adopted for the identification of critical infrastructures and vulnerabilities stage of risk management. The same modelling techniques (empirical – 23 approaches, and network – 26 approaches) also feature more than others in the risk assessment stage. For risk management implementation stage, and with specifics to the risk prioritisation sub-stage, empirical-based modelling (17 tools) and (agent-based modelling (12 tools) are the two tops modelling techniques. The control implementation sub-stage sees empirical-based (18) and network-based (13) to feature more. However, the effectiveness evaluation stage of risk management indicates quite a different outlook. Agent-based modelling technique (9 tools) appear to feature as the most used modelling techniques. We note that based on the modelling techniques, more numbers of CIP approaches feature for a combined risk identification and assessment than in the stages of prioritisation, control implementation and effectiveness evaluation combined.

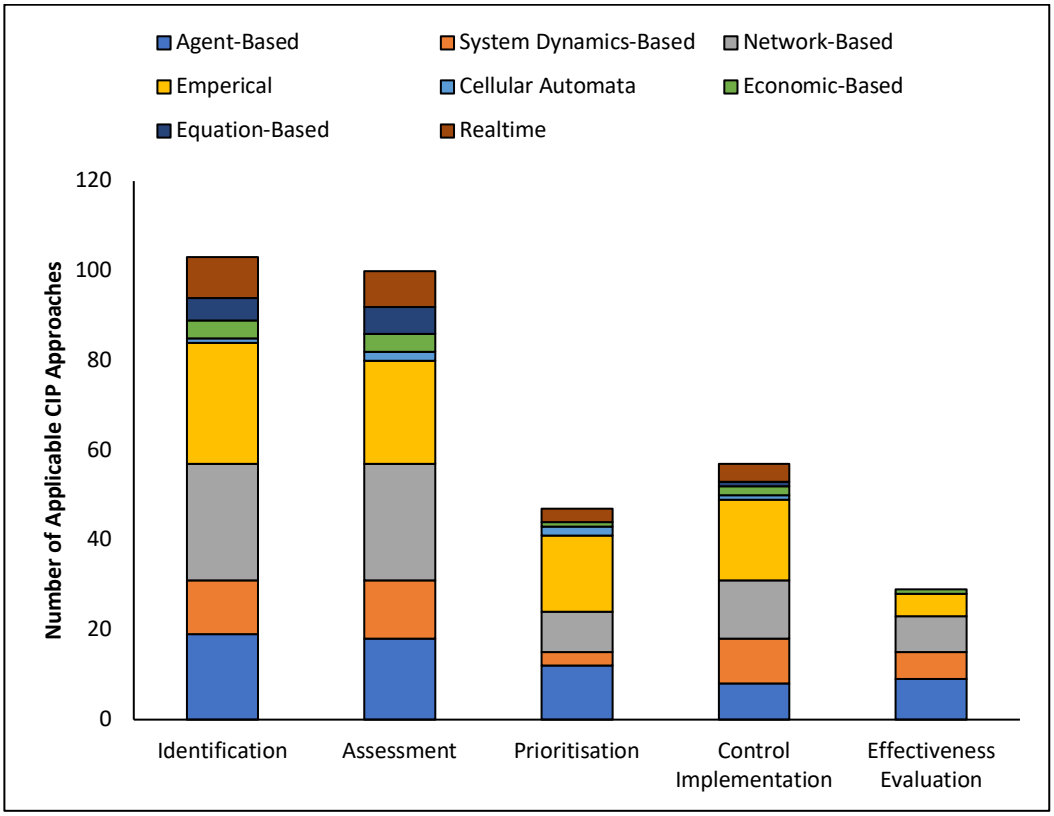


*Figure 11: Risk Stage and Modelling Techniques Analysis*

## 4.7 Resilience, Dependency and Policy and Regulations Coverage

Having underscored the significance of interdependency, resilience, and policy and regulations characteristics in CIP, the reviewed CIP approaches are analysed with respect to the coverage or inclusion of characteristics. By this, the study seeks to identify (where available) possible gaps and limitations that relate to the absence of the features in existing CIP approaches, and possibly using such information to drive suggestions of development requirements for future and improved CIP approach.

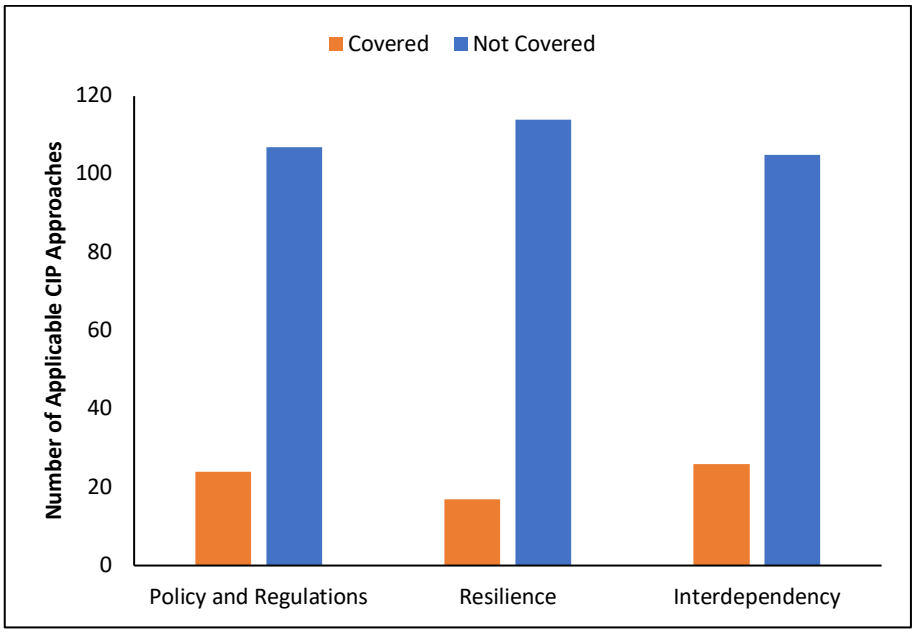


*Figure 12: Analysis of Dependency, Resilience, and Policy Characteristics*

For the resilience coverage analysis indicated in Figure 12, only 18 (nearly 14%) out of the 131 CIP approaches clearly considered an aspect of resiliency feature in their modelling or application. These included: BIRR, CIMS, CIPMA, DECRIS, EURACOM, FAIT, Fort Future, IIM, LogiSims, MBRA, DUTCH NRA, HAZOP, Risk Maps, RAMCAP-Plus, Sandia Risk Assessment Methodology, NIPP-RMF, and RMCIS. We assume that the non-coverage of resilience by a greater proportion of CIP approaches may be associated to either (i) the core objectives of their developments, which relates to perceived requirements for protecting critical infrastructures, or (ii) the development time for the tools which may have predated the concept of resilience in critical infrastructures – CI resilience not clearly defined and not gained wide attention. For the CIP tools that have considered resilience, they typically emerged in response to challenges with trends like convergence and hyper-connectivity – causing resilience to be viewed as a necessary objective.

For (inter)dependency characteristic, only 28 (representing nearly 21%) of the total CIP approaches considered some aspects of the feature in their modelling process. Some of the approaches that explicitly defined and captured interdependency features of CIs include: AIMS, Athena, CASCADE, CI3, CIMS, CIDA, CIMSuite, CIPMA, CISIA, COMM-ASPEN, IEISS, IIM, IRRIIS, MUNICIPAL, N-ABLE, NEMO, NEXUS Fusion Framework, WISE, DEW, EAR-PILAR, LUND, MIA, UIS, TIMQAV-CIS, HM-BRMCI, and QMACSR-SCADA Systems. Again, the reason for considering dependencies may be linked to the core objectives for developing some of these tools having acknowledged the significance of interdependencies for both constructive and destructive impacts on critical infrastructure operations. Behavioural, cascading effects for functions and failures appear to be at the core of the objectives for developing these approaches. For one, the acknowledgement of the link and inter-workings amongst multiple critical infrastructures became clearer much earlier than resilience.

Only 24 (representing close to 18%) of the CIP approaches indicated to support the objective of formulating policies and regulations for decision-making. These include: Athena, CIMS, CIP/DSS, CIPDSS-DM, CIPMA, Fort Future, IEISS, IIM, Knowledge Mgt & Visualisation, N-ABLE, TRAGIS, DUTCH NRA, EAR-PILAR, GAMS-CERO-ERA, CERT Initiatives, HAZOP, Infrastructure Disruptions, MARGERIT V2, MIA, OGC CIPI, PCI-Information, Risk Maps, SAIV, and UML-CI. For multi-factor coverages, only 7 (about 5.3%) of the reviewed CIP approaches considered both policy and resilience factors. These include: CIMS, CIPMA, Fort Future, IIM, DUTCH NRA, HAZOP, and Risk Maps. Similarly, only 7 (also 5.3%) of sampled CIP approaches considered both policy and (inter)dependency factors. CIP approaches in this group include: CIMS, CIPMA, IEISS, IIM, N-ABLE, EAR-PILAR, and MIA. However, only 4 (about 3.1%) of sampled CIP approaches considered both resilience and (inter)dependency factors. In the same vein, these same approaches are those that consider all factors (policy, resilience, and interdependency).

*Table 1: Criteria Meta-Data Analysis of CIP Approaches*

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| ACT | ■ | ■ | | ■ | | | ■ | | | | ■ | | | | ■ | | ■ | ■ | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | ■ | ■ |
| ActivitySim | ■ | ■ | | | | ■ | | | | | | | | | | ■ | | | | | | | | | | | | | | ■ |
| ADVISE | ■ | ■ | | | | ■ | | | | | | | ■ | | | | | | | | ■ | | | | | | | | | ■ |
| AIMS | ■ | ■ | | | | ■ | | | | | | | | | | ■ | | | | | ■ | | | | | | ■ | | ■ | ■ |
| AIMSUN | | ■ | | ■ | | | ■ | | | | | | | | | | | | | | | | | | | ■ | | | | ■ |
| AMTI Loki Toolkit | | ■ | | | ■ | | | ■ | | | | | | | | | | | | | ■ | ■ | | | | ■ | | | | ■ |
| AT/FP | ■ | ■ | ■ | | | ■ | | | | | | | | | | | | | ■ | ■ | | | | | ■ | ■ | | | | |
| ATAV-SCADA | ■ | | | | | | | ■ | ■ | | | | | | | | | | | | ■ | | | | | | | | | |
| Athena | | ■ | | | | | | ■ | | | | | | | ■ | ■ | ■ | ■ | ■ | | ■ | ■ | | | | ■ | ■ | ■ | ■ | ■ |
| ATOM | ■ | ■ | | ■ | ■ | | | ■ | | | | | | | | | | | | | | | | | | ■ | | | | |
| BIRR | ■ | ■ | ■ | ■ | ■ | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | |
| BLDMP | ■ | ■ | | | | | ■ | | | | | | | | ■ | | ■ | | | | ■ | | | ■ | | | ■ | ■ | | ■ |
| BMI | ■ | ■ | | ■ | | | | | | | | | | | | ■ | ■ | | ■ | | | | | | ■ | | | | | |
| CAPRA | | ■ | ■ | ■ | | | ■ | | | | | | | | | | | | | | | ■ | | | ■ | ■ | ■ | | | ■ |
| CARVER2 | ■ | | ■ | | | | | | ■ | | | | | | | | ■ | | | | | | | | ■ | | | | | ■ |
| CASCADE | ■ | ■ | | | | | | ■ | ■ | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| CEEESA | ■ | ■ | | ■ | ■ | | | | | | ■ | | | | | | | | | | ■ | ■ | | | | | | | | ■ |
| CERT Initiatives | ■ | | ■ | ■ | | | | | | | | | | | | ■ | ■ | | | | | | | ■ | | | | | ■ | |
| CERT/CSIRT | ■ | | ■ | ■ | | | | | ■ | | | | | | | ■ | | | | | | ■ | | | | | | | | |
| CI3 | | | ■ | | ■ | | | | | | | | | | ■ | | ■ | | | | ■ | | | | | | ■ | ■ | | ■ |
| CIDA | | | ■ | ■ | ■ | | | ■ | ■ | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| CIMS | | ■ | ■ | ■ | ■ | ■ | | | | | | | | | ■ | ■ | | | | | ■ | | | | ■ | ■ | | | | ■ |
| CIMSuite | ■ | ■ | | ■ | ■ | | ■ | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| CIP/DSS | ■ | | ■ | ■ | ■ | | ■ | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| CIPDSS-DM | ■ | | ■ | ■ | ■ | | | | ■ | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| CIPMA | | | | ■ | ■ | | ■ | | | | | | | | ■ | | | | | | ■ | ■ | | | | ■ | | | ■ | ■ |
| CISIA | | | ■ | ■ | | ■ | | | | | | | | | ■ | | ■ | | | | ■ | | | | | | ■ | ■ | | ■ |
| COMM-ASPEN | ■ | ■ | | | ■ | ■ | | | | | | | | | ■ | | | | | | ■ | ■ | | | | | | | | ■ |
| CORAS-BRA-SCADA | ■ | | | | | | | | ■ | | | | ■ | | ■ | | ■ | ■ | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | ■ | |
| COUNTERACT | ■ | ■ | ■ | ■ | ■ | | | | | | | | | ■ | | | | | | | ■ | | | | ■ | ■ | | | | |
| CSASG-SCADA Systems with Game Models | ■ | ■ | | ■ | | | | | ■ | | | | | | | | | | | | ■ | | | | | | | | | |
| CSRA-NPP | ■ | ■ | | ■ | | | | ■ | ■ | | | | | | | | | | | | | | | | | | | ■ | | |
| CSRAM-ICSP | ■ | ■ | | ■ | | | | ■ | ■ | | | | | | | | | | | | | | | | | | | ■ | | |
| Cy-T SCADA RF | ■ | ■ | | ■ | | | | | ■ | | | | | | ■ | | ■ | ■ | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | ■ | |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| DECRIS | ■ | | ■ | ■ | ■ | | | | | | | | | ■ | ■ | | | | | | ■ | | | | | ■ | ■ | | ■ | |
| DEW | ■ | ■ | ■ | | | | | ■ | ■ | | | | | | | | ■ | | | | ■ | | | | | | | | | ■ |
| DMRIM-SCADA System | ■ | | | | | | ■ | | ■ | | | | | | ■ | | | | | | | | | | | | | | | |
| DUTCH NRA | ■ | ■ | ■ | | | | | | | | | | ■ | | | ■ | | | | | ■ | | | ■ | | ■ | ■ | | | |
| EAR-PILAR | ■ | ■ | ■ | ■ | | | | | ■ | | | | | | | ■ | | | | | | | | ■ | | | | | ■ | ■ |
| ECI-GIS | ■ | ■ | | | | | | | | | | | ■ | | | ■ | | | | | | ■ | | ■ | | | | | | ■ |
| EMCAS | ■ | ■ | ■ | | | ■ | | | | | | | | | ■ | | | | | | ■ | ■ | | | | | ■ | | | ■ |
| EpiSimS | ■ | ■ | | | ■ | ■ | | | | | | | | | | | | | | | | | | | ■ | | | | | ■ |
| EPRAM | | ■ | ■ | | | | | | | ■ | | | | | | | | | | | ■ | | | | | | | | | |
| ERC-SCADA System-Petri Net Analysis | ■ | ■ | | | | | ■ | | | | | | | | | | ■ | | | | ■ | | | | | | ■ | | | |
| EURACOM | ■ | ■ | ■ | ■ | ■ | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | |
| FAIT | ■ | ■ | | | | | | ■ | | | | | | | | | | | | ■ | ■ | ■ | | | | ■ | | ■ | | ■ |
| FastTrans | ■ | ■ | ■ | | | ■ | | | | | | | | | | | | | | | | | | | | ■ | | | | ■ |
| FEPVA | ■ | ■ | | | | | | ■ | | | | | | | | | | | | | ■ | | | | | | | | | |
| FINSIM | ■ | ■ | | | | ■ | | | | | | | | | ■ | | | | | | ■ | ■ | | | | | | | | ■ |
| FMEA/FMECA | ■ | ■ | ■ | | | | | | ■ | | | | | | | ■ | ■ | | | | | ■ | | | | | | | ■ | |
| Fort Future | ■ | ■ | ■ | | ■ | ■ | | | | | | | | | ■ | ■ | ■ | ■ | ■ | | ■ | ■ | | | ■ | ■ | ■ | ■ | ■ | ■ |
| FTA | ■ | ■ | ■ | | | | | | ■ | | | | | | | ■ | ■ | | | | | ■ | | | | | | | ■ | |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| GAMS-CERO-ERA | ■ | ■ | ■ | ■ | | | | | | | | | ■ | | | ■ | | | | | | ■ | | ■ | | | | | | |
| GIS Interoperability | | | ■ | | ■ | | | | | | | | | | | | | | | | | | | | | ■ | | | | |
| GoRAF | | ■ | ■ | ■ | | ■ | | | | | | | ■ | | | ■ | ■ | | | | ■ | | | | | | ■ | | | ■ |
| HAZOP | ■ | ■ | ■ | | | | | ■ | ■ | | | | | | | ■ | ■ | | | | ■ | | | ■ | | | | | ■ | |
| HCSim | | ■ | | | | ■ | | | | | | | | | | | | ■ | | | | | | | ■ | | ■ | | | ■ |
| HM-BRMCI | ■ | ■ | | ■ | | | | ■ | | | | | | | ■ | | ■ | ■ | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | ■ | ■ |
| HURT | | ■ | ■ | ■ | | | | | ■ | | | | | | | | | | | | | | | | ■ | | | | | |
| HYDRA Pop & Eco Modeling | | ■ | | | | | | ■ | | | | | | | | | | | | | | ■ | | | ■ | | | | | |
| I2SIM | ■ | | | | | | ■ | | | | | | | | | ■ | ■ | | | | | | | | ■ | ■ | | | | ■ |
| ICS-CDTP | ■ | ■ | ■ | ■ | | | ■ | ■ | | | | | | | ■ | | ■ | ■ | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | ■ | |
| IEISS | ■ | | ■ | ■ | | ■ | | | | | | | | | | | | | | | ■ | | | | | | ■ | ■ | | ■ |
| IIM | ■ | | ■ | ■ | | | | | | | ■ | | | | ■ | | | | | | ■ | ■ | | | | ■ | ■ | | ■ | ■ |
| Infrastructure Disruptions | | | | ■ | ■ | | ■ | | | | | | | | | ■ | | | | | | | | ■ | | | | | | ■ |
| INTEPOINT VU | | | ■ | | | ■ | | | | | | | | | ■ | ■ | | | | | ■ | | | | | ■ | | | | ■ |
| IRAM | | ■ | ■ | ■ | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | | | ■ |
| IRAM-SCADA INFORMATION Sec | | ■ | | | | | | | | | ■ | ■ | | | | | | ■ | | | ■ | | | | | | ■ | | | |
| IRRIIS | ■ | ■ | ■ | ■ | ■ | | | ■ | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| Knowledge Mgt & Visualisation | | | | ■ | ■ | | | ■ | | | | | | | | | | | | | ■ | | | | | ■ | ■ | | | ■ |
| LogiSims | ■ | ■ | ■ | ■ | | | | | ■ | | | | | | | | | | | | ■ | | | | ■ | | | | | ■ |
| LS-DYNA | ■ | ■ | | | | | ■ | | | | | | | | | | ■ | ■ | | | | | | | | ■ | | | | ■ |
| LUND | ■ | ■ | | | | | | ■ | ■ | | | | | | | | | | | | ■ | | | | | ■ | | | | |
| MARGERIT V2 | ■ | ■ | | ■ | | | | | ■ | | | | | | | ■ | | | | | | ■ | | ■ | | | | | ■ | |
| MBRA | ■ | ■ | ■ | | | | | ■ | | | | | | | | | | | | | ■ | ■ | | | | ■ | | | | |
| MIA | ■ | ■ | | | | | | | ■ | | | | | | | | ■ | | | | ■ | | | ■ | | | | | ■ | |
| MIITS | ■ | | | | | ■ | | | | | | | | | ■ | | | | | | | | | | | | | | ■ | ■ |
| MIN | ■ | | | | | ■ | | | | | | | | | | ■ | | | | | | | | | | ■ | | | | ■ |
| Modular Dynamic Model | | ■ | | ■ | ■ | | ■ | | | | | | | | | | | | | | ■ | | | | | | | | | ■ |
| MSM | ■ | ■ | ■ | | | | | ■ | | | | | | | | | | | | | ■ | | | | ■ | | ■ | | | |
| MUNICIPAL | ■ | | ■ | | | | | ■ | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | ■ | ■ |
| N-ABLE | ■ | | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | | ■ | ■ | | | | ■ | | | | ■ |
| NEMO | | | ■ | ■ | ■ | | | ■ | | | | | | | ■ | | | | ■ | | ■ | | | | | ■ | ■ | | | ■ |
| Net-Centric GIS | ■ | ■ | | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | ■ | | | ■ |
| NEXUS Fusion Framework | | ■ | | | | ■ | | | | | | | | | ■ | ■ | | | ■ | | ■ | | | | | ■ | | | | |
| NG Analysis Tools | ■ | ■ | | | ■ | ■ | | | | | | | | | | | | | | | ■ | | | | | | | | | ■ |
| NGFast | ■ | ■ | | | ■ | | | | ■ | | | | | | | | | | | | ■ | | | | | | | | | ■ |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| NIPP-RMF | ■ | ■ | ■ | ■ | ■ | | | | ■ | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | |
| NSRAM | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | ■ |
| NSRM | ■ | ■ | ■ | ■ | | | | | | ■ | | | | | | | | | | | | | | | | | ■ | | | |
| OGC CIPI | ■ | | ■ | | ■ | | | | ■ | | | | | | | | | | | | | | | ■ | | | | | | |
| PC Tides | ■ | | | | | | | | | | | ■ | | | | | | ■ | | ■ | | | | | ■ | | ■ | | | ■ |
| PCI-Information | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | ■ | | | | | | |
| PFNAM | ■ | ■ | | | | | | ■ | | | | | | | | | | | | | ■ | | | | | | | | | |
| PipelineNet | ■ | ■ | | ■ | | | | ■ | | | | | | | | | | | | | | | | | ■ | | ■ | | | ■ |
| PMU-Based RAFPCS | ■ | ■ | | ■ | | | | ■ | | | | | ■ | | | | | | | | ■ | | | | | | | | | |
| QCRREM | ■ | ■ | | | | | | | ■ | | | | | | | | ■ | | | | | | | | | | ■ | | | |
| QCSRAM-SCADA | ■ | ■ | | | | | | | | | ■ | | | | | | | | | | ■ | | | | | | | | | |
| QMACSR-SCADA Systems | ■ | ■ | | | | | | | | | | ■ | | | | | | | | | ■ | | | | | | | | | |
| QTRIM | ■ | ■ | | | | | ■ | | | | | | | | ■ | | ■ | | | | ■ | | | | | | ■ | | ■ | |
| QualNet | ■ | ■ | | | | | | ■ | | | | | | | ■ | | | | | | | | | | | | | | | ■ |
| R-NAS | ■ | ■ | | ■ | ■ | | | ■ | | | | | | | | | | | | | | | ■ | | | ■ | | | | ■ |
| RA-GPS-SCADA-R | | | | | | | ■ | | | | | | | | | | | | | | | | | | | | | | | |
| RA-SCADA Railways | | ■ | | ■ | | | ■ | | | | | | | | | | | | | | | | | | | ■ | | | | |
| RADR | ■ | ■ | | ■ | | | | | | | | ■ | | | ■ | | | | | | | | | | | | | | | ■ |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| RAIM | ■ | ■ | | ■ | | | | | | | | | ■ | | | | | | | | ■ | | | | | | | | | |
| RAMCA | ■ | ■ | | | | | | | | | | ■ | | | ■ | | | | | | | | | | | | | | | ■ |
| RAMCAP-Plus | ■ | ■ | ■ | ■ | | | | | ■ | | | | | | | ■ | ■ | | | | ■ | | | ■ | ■ | | | | | |
| Restore | | | ■ | | | | | | ■ | | | | | | | | ■ | | | | ■ | | | | | | | | | ■ |
| Risk Maps | ■ | | | | | | | | | | | | | | | ■ | ■ | | | | ■ | ■ | | ■ | | ■ | ■ | ■ | ■ | |
| RMGCIS | | ■ | | ■ | | | | | ■ | | | | | | | | ■ | | | | ■ | | | ■ | | | | | | |
| RTDS | ■ | | | | | | | | | | | | ■ | | | | | | | | ■ | | | | | | | | | ■ |
| RVA | | ■ | | | | | | | ■ | | | | | | ■ | ■ | | | | ■ | | ■ | ■ | | ■ | | | | | |
| SAIV | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | ■ | | | | | | |
| Sandia Risk Assessment Methodology | ■ | ■ | | ■ | | | | | | | | | ■ | | | | | | | | | | | ■ | | | | | | |
| SC-Based ARAC | ■ | ■ | | | | | | | | | | ■ | | | | | | | | | | | | | | | | ■ | | |
| SessionSim | ■ | | | | | ■ | | | | | | | | | ■ | | | | | | | | | | | | | | | ■ |
| SIERRA | ■ | ■ | | ■ | ■ | | | ■ | | | | | | | | | | | | | | | | | | ■ | | | | ■ |
| SRM-ICSP | ■ | ■ | | | | | ■ | ■ | | | | | | | | | | | | | | | | | | | | ■ | | |
| TEVA | ■ | ■ | ■ | | | | | | ■ | | | | | | | | | | | | | | | | ■ | | ■ | | | ■ |
| TIMQAV-CIS | ■ | ■ | | | | | | ■ | | | | | ■ | | ■ | ■ | ■ | | | | ■ | | | | | | ■ | | | |
| TRAGIS | ■ | | | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | ■ | | | ■ |
| TranSims | | | | | ■ | ■ | | | | | | | | | | ■ | | | | | | | | | | ■ | | | | ■ |

| CIP Tools / Techniques (Methodologies) | Risk Management stages | | | | | Modelling Techniques | | | | | | | | | Critical Infrastructure Sectors | | | | | | | | | | | | | | | | | Software Tool Support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Identification | Assessment | Prioritisation | Control Implementation | Effectiveness Evaluation | Agent-Based | System Dynamics-Based | Network-Based | Empirical-Based | Cellular Automata | Economic Theory-based | Equation-based | Real-Time Simulation | Methodology (No Modelling) | Chemical | Commercial Facilities | Industrial Control | Dams | Defence Industries | Emergency Services | Energy | Financial Services | Food & Agriculture | Government facilities | Health & Public Health | Transportation System | Water & Waste Water | Nuclear | IT & Telecommunications | |
| UIS | ■ | ■ | ■ | ■ | | ■ | | | | | | | | | | ■ | | | | | | | | | | ■ | ■ | | ■ | ■ |
| UML-CI | ■ | | | | | | | | | | | | ■ | | | | | | | | | | | ■ | | | | | | |
| UPMoST | ■ | | | | | | | | | | | | | ■ | | ■ | | | | | | | | | | | | | | ■ |
| USArmy Risk Mitigation | | ■ | | ■ | ■ | | ■ | | | | | | | | | ■ | | | ■ | | | | | | | | ■ | | | ■ |
| VACSPI | | ■ | | | | | | | | | | ■ | | | | | | | | | ■ | | | | | | | | | |
| VAM-SCADA Security | ■ | | | | | | | | ■ | | | | | | | | | | | | ■ | | | | | | | | | |
| VINCI | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | | | | | | ■ | |
| VISAC | ■ | ■ | | | | | ■ | | | | | | | | ■ | | | | | | | | | | | | | ■ | | ■ |
| WISE | ■ | ■ | | ■ | ■ | ■ | | | | | | | | | | ■ | | | | | | | | | ■ | | ■ | ■ | | ■ |

# 5 Discussion of Findings and Conclusions

In this section, a discussion is presented based on the results of reviewing the CIP approaches. To simply understanding, the discussions are presented in line with the research questions outlined in section 1.3.

## 5.1 Discussions

### 5.1.1 – RQ1: What are the common CIP approaches (Tools and Techniques) available for the management of security risk?

On the above question, it is found that there is a vast number of CIP approaches that exist either as tools, techniques or methodologies. As shown, *some of the CIP approaches, especially the tools; are more fittingly designed or developed for operations and performance modelling and simulations, than for specifically for security. However, such tools can be used to underscore security-related attributes.* For instance, the modelling of system components, their functionality and performances can provide a good platform for evaluating the impact of security feature or the lack of, within critical infrastructure set-ups.

As security concerns for critical infrastructures continue to increase, analysts, experts, users, and national security outfits related to affected critical sectors will continue to adopt methods, as well as seek newer approaches that suite their peculiar environments and security needs to ensure that their critical infrastructures are protected. The result is the proliferation of these CIP tools across varied sectors that constitute critical infrastructures. *A common feature that seem to surface amongst the various CIP approaches is that they are all based on risk management. However, it is possible to distinguish CIP approaches based on the scope or stage of overall security risk management functions considered or reflected in each approach*.

### 5.1.2 – RQ2: Which are the common modelling techniques applied in CIP approaches?

On the above question, it is discovered that a variety of techniques have been used for modelling and simulating CIP. *The common techniques with wide interests and adoptions include: agent-based, system dynamics-based, network-based, empirical-based.* These do not represent the only applicable techniques for modelling as developments continue to emerge, they only represent those more commonly defined and used. Newer techniques may be defined building from the combination of two or more of the presented techniques or even totally new modelling paradigms for accomplishing any intended goals and objectives.

Based on analyzed results, it is suggestive that the development of CIP approaches appears to be more widely employed using the techniques listed. Of these, *the empirical-based model seems to be most widely employed for CIP research and the development of security approaches.* This is closely followed by network-based and system dynamics-based modelling techniques. It would seem that the preferences for empirical-based models may be linked to the growing Big data trends. This reflects the increasing desire to understand and analyze CI security using real or actual historic data and drawing from expert knowledge and experiences. Thus, the growing inclination to this modelling technique may well be associated to its ability to provide actual scenario data from which real analysis and insights may be achieved. It supports the notion of system, data, and results fidelity in modelling and simulation, which seem to be a growing interest. Fidelity emphasizes the ability

and extent to which a true representation of a system phenomenon is capture and used to provide insights and drive decision-making. This attribute cannot be overemphasized within critical infrastructures and effective security in particular; since the true nature of CI phenomena may not be better captured but from realistic data records. In using stored historic data, it becomes easier to observe and connect the interrelationships and interdependencies among critical infrastructure components, system and sectors. Thus, empirical-based modelling technique for CIP seem to better support identifying more recurrent, realistic and suggestive failure patterns, quantifying interdependency-related indicators for risk mitigations, support emergency decision-making and provide validation parameters to support other modelling techniques [16]. Notwithstanding, the empirical-based model is not without limitations, some of which include report bias and non-standardized data collection. These makes the case for the usefulness of other modelling techniques such as network-based, agent-based, system dynamics-based modelling, etc.

Network-based modelling is also a widely adopted approach, perhaps because of its ability to support the modelling of interdependencies among CI systems, especially within a localized domain. Thus, it is easier to draw insights relating to CI representations along topological or flow pattern analysis and the evaluation of cascading impacts. Agent-based and system dynamics-based modelling are also quite acknowledged and used in CIP simulation, especially for modelling discrete events related to infrastructure performances in emergencies and human behavioral predictions. Agent-based modelling is weak in that its application is often highly reliant on the assumptions of the modeler which are sometime difficult to justify [16]. System dynamics-based modeling also struggle with effectively analyzing component-level dynamics because of the multiple computation procedure involved. However, real-time modelling capacity is a feature that appear desirable as some of the tools classed under other modelling techniques (empirical-based, network-based, and agent-based) also include real-time features, enabling for the recurrent representation and update of behavioural dynamics as they occur with minimal delays. This is quite necessary to be able to keep tabs and timely address the sensitivity and criticality of security risks in critical infrastructures.

As the emphasis on fidelity, dependency and resilience of CIS continue to rise, we think that increased interests and support will tend towards empirical-based modelling, with progressive support for network-based, agent-based, and system dynamics-based modelling. The less emphasis on the other modelling techniques (equation-based, economy-based, etc.) indicates that these methods are either too complex to adopt or use, or the lack of popularity of their generalized concepts in relations to CI modelling.

#### 5.1.3 – RQ3: What is the most application mode for existing CIP approaches?

In answering the third research question indicated above, it is found that there are two major application modes for existing CIP approaches. The first mode is that CIP approaches may exist as software tools that can be deployed on computing platforms and used to further intended security functions in part or full. This typical represents an advanced or progressive development life cycle state of a CIP from a methodology state. Secondly, CIP approaches may also exist as working methodologies proffering conceptual, theoretical descriptive stages and process guidelines to be engaged via external efforts and assistance to achieve similar protection for CIs.

Typical CIP functions that are furthered by software-based tools range from asset characterization (e.g., EAR-PILAR, GoRAF) threat, vulnerability and risk analysis, (inter)dependency analysis, policy implementation (e.g., AIMS, Athena, CASCADE, CARVER2, CIP/DSS, TEVA, etc.), damage/impact analysis and prediction (e.g., ECI-GIS, WISE), failure analysis (e.g., NSRAM), sensitivity analysis for

decision-support (e.g., NEMO). The non-software-based approaches typically exist as working methodologies, and also capture similar contexts and functions as the software-based tool. However, the non-software-based approaches appear to be chiefly contextualized around functionalities related to the management of networks, risks, impacts, or dependencies. Some specific function examples include: failure/incident analysis and management (e.g., FMEA-FMECA, CERT/CSIRT, FTA, OGC CIPI), Multi-criteria decision-making for risk analysis and reduction (e.g., GAMS-CERO-ERA, DUTCH APPROACH, HAZOP), Component/system relationship (network) mapping (e.g., LUND, MARGERIT, etc.), and interdependency analysis (e.g., MIA)

Based on the results obtained, we find that more than half of the CIP approaches surveyed appear to have resulted in the development of computer-based platforms (software tool) for either commercial or restricted uses. Restrictions range from military, institutional, corporate or private uses. This reflects a steady and increasing interest and trend towards translating or extending conceptual designs and workflows of CIP approaches into program (software) executables on computing platforms for automated executions. This is a positive and welcomed trend as it bears the benefit of facilitating speedy process executions while reducing the potential for human-generated errors and delays. Suggestively, a motivation for this can perhaps be attributed to the need to simplify or reduce the complexity, difficulty and time-scale involved in manually applying security modelling processes on CI environments. These domains typically comprise of huge number of components, processes, and interactions that often span more than one geographical area. Automating the manual processes via software essentially helps to speed up security modelling processes, as well as concurrent applications across multiple sectors to support timely decision-making.

### 5.1.4 – RQ4: What sectors are the CIP approaches chiefly applied?

In answering the fourth research question indicated above, it is discovered that CIP modelling approaches are applied to several sectors or domains of a country's economy. There seem to be a very wide interest and research in the energy sector. This sector encompasses electricity, pipeline and oil, and natural gas CIs. There is also a significant interest in the water and waste water, transportation, chemical, and industrial CI sectors. Most of these sectors fall within the category of CNIs defined in the UK CPNI documentation [13].

Particularly, the importance and value of sectors such as energy and transportation as critical national infrastructures (CNIs) is noted. For example, the energy sector is quite critical perhaps because of the level of dependency of several other critical infrastructures on the energy sector. All of the other CIs require some form of energy source and rely on an energy sub-sector for power to drive its functionalities. Thus, the energy sector takes on a very critical, if not indispensable; position and role within critical infrastructure interdependencies. An attendant energy sub-sectors become critical to the operations of other connected and dependent infrastructures. The consequences or impact of the failure of the energy infrastructure, can inevitably ripple through and affect other dependent infrastructures, causing a myriad of cascading damaging outcomes (physically, operationally, and economically) through a chain of interdependent CIs with a nation or global social ecosystem. This may also explain why there are more interests, studies, and efforts towards providing more secure energy sector solutions, and with continuous improvements.

However, it is interesting to note that sectors such as emergency services, food &. Agriculture, dams, and defense industries have quite few interests and research attention - at least as reflected in the results. We reckon that this may be because these sectors often appear at the end of CI

interdependency chains, and do not always bear very direct and immediate social large-scale consequences and impacts when compromised. More so, research and developments in the area of CIP appear to follow similar direction as the trends of malicious activities and events experienced. The sectors in question do not seem to fall amongst those most predominantly plagued with increasing threats and attacks. At least there are fewer records of CI incidents and failures related to emergency services, dams or food and agriculture sectors compared to the energy and transport sectors. While it might seem reasonable to focus greater solution efforts where there are greater threats and risk challenges, the possibilities for common cause failures are very imminent, hence, requires that a good measure of attention be given to other supporting CI sectors.

### 5.1.5 – RQ5: What stages of risk management are aptly covered by the CIP approaches?

In answering the fifth research question indicated above, it is found that empirical-based, network-based, and agent-based modelling techniques appear to be most widely used techniques in the risk management framework stages. System-dynamics-based techniques are typically used for simulating continuous system behaviours such as estimating the effectiveness of implemented procedures in critical infrastructures. A consistent pattern is observed which suggests that empirical-based modelling is more widely employed in risk identification, assessment, prioritisation and control implementations stages, and not much considered in effectiveness evaluations. Network-based modelling also see wide acceptance in risk identification, assessment and control implementation. This may be because network-based techniques which include either topology-based or flow-based methods are quite supportive for capturing interdependency characteristics (layered connection and flow) and descriptions of CIs, identification of critical components along with suggestions for emergency protection and response improvements [16].

In general, there seems to be greater interests and momentum on researches around risk identification and assessment. Results also indicate that the third aspect of interest in security risk management stages seem to be control implementation. Aspect of risk prioritisation and effectiveness evaluation do not seem to enjoy much attention and research like the prior stages. These give an indication of the aspects of security risk management where the most interests are channelled, and where the direction of CIP developments trends seem to focus. It shows that beside identifying and assessing security risks on CIs, the next thing in the minds of CI owners/users is what controls to implement to mitigate or eliminate characterised risks. The outlook of results indicates that this venture is viewed as more important than first understanding the varied criticality levels of security risks and devising a strategy for implementing controls to yield the highest possible security and resilience outcome. Even less acknowledged is the value of evaluating the extent to which desired CI protection is achieved post control implementation to provide success measures and potential guidance for further improvements. More common is the issue/debate around the variability of approaches for measuring risks, and how such measures reflect true situations of the system involved.

### 5.1.6 – RQ6: What CIP approaches consider resilience, (inter)dependency and policy formulation factors, and what is the general consideration level of these three attributes in reviewed CIP approaches?

In providing answer to the sixth research question as mentioned above, it is found that very few (less than one-fifth) of the CIP approaches considered resilience as important. More focus and purpose-development emphasis seem to incline towards capacities for guarding against the

occurrence of malicious attacks or compromises on CI components and sectors. Capacities that may help reduce attack impacts and sustain operations or functionalities during and after malicious compromises do not seem largely considered. Perhaps this may be because most CIP approaches are pretty older than the trend of resilience (i.e., were already in use prior to when resilience became a feature of significance and concern) and there have not been newer or updated versions of these approaches. Alternatively, the significance of resilience may also not have been clearly understood by developers as at the time of developing some of the approaches, which makes for why resilience feature is not reflected in the tools.

Besides engaging protective efforts to guard against malicious intrusions and compromises of CIs, the need to engage and ensure the capacity to continue or sustain operations – providing the needed services while under attack or managing the attacks is ever important. For some of the critical national infrastructure sectors, a disruption or its cascading effect is not a welcome phenomenon. Anticipation, absorption, adaptation and rapid recovery are very essential sub-features of resilience [58]. While newer approaches are being conceived with the necessary features, it is expected that the older CIP approaches will also see appropriate modifications to include resilience where missing, just as in the case of NIPP-RMF which earlier versions did not consider resilience but now revised in 2013 to include both security risk and resilience characteristics.

Although not a very wide acceptance and inclusion of (inter)dependency characteristic is seen in the reviewed CIP tools, its coverage seem slightly more than resilience. Some modelling dimensions covered include: Component/infrastructure-level (e.g., AIMS, MUNICIPAL), operational/functional-level (e.g., CASCADE, CIPMA), vulnerability-level (e.g., MIA), Cost/Time-dependencies (e.g., CI3), and market effects, (e.g., CommAspen). The results indicate a gradual acknowledgement of the importance of interdependencies in the modelling and analysis of CIP. Private and public CI owners and operators are beginning to recognize that understanding the relationship amongst CI components and systems can greatly support a better attainment and enhancement of security and resilience.

It is also found that less than one-fifth of the CIP approaches clearly indicate the formulation of policy and regulations as part of the objectives for their development or use. Most of the objectives are directly focused on either the assessment of risks related to threats, vulnerabilities, and impacts, or the modelling of system behaviours to understand operational or failure impacts along with dependencies involved. Again, these approaches are mostly emerging from research institutes and academic institutions rather than government regulatory agencies. It also indicates that the domain of CIP is much more characterised with self-garnered protective solution ventures than in compliance-based approaches. This disparities and uniqueness of security problems, security requirements and needs may be behind the trend where infrastructure organisations and sectors develop and adopt protection techniques that are rather tweaked to their specific environments.

From a multi-factor coverage perspective, we find that very few CIP approaches currently retain considerations for policy, resilience, and interdependency factors. In precise terms, only CIMS, CIPMA, and IIM appear to satisfy these criteria. Interestingly, none of these approaches adopt the emerging empirical or network-based modelling techniques. Rather, these follow agent-based and system dynamics modelling. CIP approaches such as; DUTCH NRA, HAZOP, and Risk Maps are additional CIP methodologies without software support which cover aspects of policy and resilience alone. IEISS, N-ABLE, EAR-PILAR, and MIA are other additional CIP approaches that consider only policy and (inter)dependency factors. This brings to bare the limitations of existing CIP approaches

to sufficiently address the dynamics of protection in modern CI. The level of multi-factor coverage is significantly low compared to the proportion of CIP approaches being developed. This also points to the need to upgrade or refine existing approaches to incorporate any of the three factors lacking in order to improve the protection capabilities of the tools or methodologies.

## 5.2 Summary and Recommendations

### 5.2.1 Summary

Existing approaches for modelling and simulating CIP appear to principally focus on the study and modelling of large-scale infrastructures, their dynamic behaviours, interrelationship, and interdependency scenarios. Most attentions and research interest coverage seem centred on infrastructures classified by policy to be under the category of *'critical national infrastructures' - CNI*. Typical contexts dominantly characterising the objectives for the development of CIP modelling approaches reflect some very clear trends. One of these inclines towards the efforts at determining the dynamic behaviours of CI systems using modelling techniques such as agent-based, system dynamics-based, network-based, empirical-based techniques. These techniques provide the means to identify and characterise the causes of instabilities (anomalies and disruptions) within CI setups through recognising critical hazards and risks, their interdependencies, scale of destructive impacts and associated cascade. In relations to security and protection of CIs, each of these techniques enable distinctive capacities to examine and observe the effects of security-related events and incidents. They also support understanding how such impacts on normal functionality and operations of critical infrastructure across chains of dependencies.

Essentially, the protection of CIs is wrapped around the techniques for modelling and analysing security-related operations, activities and stages of risk management, and mostly within the confines of specific infrastructure environments and sectors. Empirical-based and network-based modelling techniques are gaining wider interests and adoption for studying/exploring the protection of CIs. This may be connected to the growing emphasis on the significance interdependency analysis and high-fidelity representation of model structures and outputs in CIs. This is a clear shift from initial attractions to agent-based and system dynamics-based techniques. In particular, empirical-based modelling combined with risk identification, assessment, implementation and management of risk are among the most common implementations. This is occasioned by the growing adoption and use of setups and models that generate or feed-on actual scenario data or its nearest representation to support infrastructure sensitivity analysis for decision-making.

From the generality perspective of risk management coverage, the NSRAM and NIPP-RMF are two common methodologies noted to be quite encompassing in their scope consideration of typical risk management stages and activities. As it appears, NIPP-RMF in particular is noted to be by far the most common, most updated, and most advanced CIP plan going by its objectives, strategies and organisation; a point also agreed by other security researchers [2]. However, NIPP-RMF exists as a methodology and does not have any tool (software) support for its application. This in itself is a shortcoming, which makes that the methodology could be complex and time-consuming to implement. Also, all risk management stages prescribed in NIFF-RMF (identification, analysis and assessment, control implementation, effectiveness evaluation) are not completely reflected in all other CIP approaches, instead, these approaches appear to be tailored to the interests and needs of specific user organisations or sectors, thus, biased to only adopt the risk management sub-stages and activities deemed relevant to the perceived threats. These scenarios may also be benefiting

from the influence of a shallow understanding of risks associated to the domain or sector inherent in those responsible.

The options are between what we consider as *'specificity'* and *'generality'* for both scope coverage for CI sectors and security risk management stages. Both of which bear their own rewards and downsides. Having security modelling tools that are more specific to CI sectors would allow for a narrower and deeper context coverage and analysis, which will mean better and more tailored solutions. Security-related attributes such as interdependencies, impacts, and scalability can be well considered and incorporated in analysis process with minimum or no assumptions. This bears the potential to improve the quality of models and results, and can encourage specialisation.

On the other hand, generality brings about a capability to apply a tool to multiple CI sectors. However, the likelihood of capturing the different possible contexts and scenarios in all the sector is greatly reduced due to the complexity involved. Where this is achieved, the application process could be time-consuming. However, one clear indication that can be immediately drawn from the results obtained is that, a holistic security modelling of CIs cannot be well attained using any single approach – a tool or technique. A combination of multiple approaches, most suggestively a tool and technique (methodology or framework) is perhaps the way to go. The combination will typically involve the abstraction of concepts into systems, methods or procedures, and can be manually or automated. The choice of approaches to combine or abstract from would depend on the security modelling goal desired and the complements provided by each. This implies that varied combinations of security modelling and simulation approaches can be explored to achieved varied CI protection objectives.

For example, the capabilities of GoRAF may be combined with concepts in NIPP-RMF to achieve a security modelling that combines agent-based with real-time modelling techniques and with software support for the process. Although GoRAF does not provision for security risk identification and effectiveness evaluation, these processes can be from the concepts in NIPP-RMF and probably explored manually. This combination provides a hybrid CIP modelling concept with the advantage of applicability to a wider scope of CI sectors with resilience capability. The downside is that interdependency and policy & regulations attributes are not explicitly covered in the hybrid concept. For this, a resolution can be achieved by combining CIMS capabilities with NIPP-RMF concepts. The hybrid output of this combination brings in interdependency, resilience, and policy & regulations attributes. It also covers a broad scope of security risk management, and a wider scope of CI sectors. Another example involves combining CASCADE capabilities with HAZOP and IRRIIS. While CASCADE brings in the strengths of a combined empirical and network-based modelling with application to at least 11 CI sectors, its limitation of not provisioning for resilience and policy & regulations is covered up by the properties of HAZOP. And of course, IRRIIS features helps to provide missing risk management contexts – prioritisation, control implementation, and effectiveness evaluations. Following the above examples, it is suggested that security model researchers and developers should first be clear and definitive about the security modelling scopes and objectives desired in a project, as this can help with the identification of the necessary features to consider in developing new approaches, or even determining what existing approaches to combine.

Another observed trend in the development of CIP approaches relates to how security risk (threats, vulnerabilities, attacks, and impacts) states of CIs are modelled and studied. Risk management methods appear to be driving the process of deriving clearer and more secure performance insights for CIs and the responses to the security risks identified. Within the concepts of security risk management, wider interests and attention seem to concentrate on the early stages; *(i)*

*identification of Critical infrastructure, hazards and vulnerabilities*, and (*ii) assessment and analysis, of security risks.* Although quite relevant and useful, these beginning stages to security risk management do not include the core of activities that establish the necessary solution to the existence or emergence of security risk. Rather, these stop at clarifying the existence and nature of risks. The two stages referred do not allow for specific action to be engaged towards active and direct control, mitigation or elimination of risks, which obviously constitutes the objective for engaging the process in the first place. An approach that includes the pragmatics of implementing the necessary control actions to curb security risk can be a better solution.

The sector with the widest attention and interest in terms of CIP is the energy sector. It is not surprising that this is the case as the energy sector encompasses multiple sub-sectors such as electricity, pipeline and oil, and natural gas. These sub-sectors embody the capacity that sustains nearly all other CI sectors. Thus, the consequences and impacts of failures and disruptions of energy sub-sectors can greatly be felt on other dependent sectors. On the other hand, the sector demonstrating least coverage is the emergency services, food and agriculture and dams. The few approaches covering these sectors are within the generality group and only hold claims of applicability for some of these sectors. Questions can arise as to the effectiveness of designated approaches in the less-responsive sectors application.

It is apparent that the nature of security risks on CI seem evolving along new trends where IoT devices and applications are being integrated into CI systems. IoT systems are typically characterised by; variability of scale in components, temporality of connections amongst devices, and the heterogeneity of actors. These attributes introduce a lot of dynamics into the system that cannot be ignored. The assessment stage/activity characterised in existing CIP tools and techniques lack the sufficient capabilities to handle such dynamics because they are designed and structured to operate statically and periodically [42], [60]. Temporality of connections occasions a high probability for loosely coupled devices to exist in CI setups. Variability of scale means a high likelihood for new systems to emerge as part of the CI network. Both scenarios can exist between periodic risk assessment without their risk impacts to the whole system being accounted for. Risk assessment would need to cater in real-time for emerging system connectivity, clearly and timely characterise the level of temporality of devices in relations to their risk impact.

Arguably, modelling for critical infrastructure protection seem not entirely new, as its underlying concepts typically bear relativity to safety modelling and analysis. What has happened is that over time, security has become quite pronounced and relevant because of technology trends such as connectivity. This has made critical infrastructure sectors easily susceptible to intentional cyber-engineered attacks. Having also become so tightly coupled and interdependent, incidents show that the compromise, disruption and failure of CIs is not only restricted to causes and vectors related to natural disasters. Human-initiated actions via technology abuse or mal-application can; and is increasingly an influencer.

However, what seems new and perhaps not well reflected – at least directly in most of the critical infrastructure modelling and security approaches (tools, techniques, and methodologies) – is the concept of addressing *'resilience'*. Most CIP approaches reviewed mainly focus on exploring concepts and phenomena related to security, reliability, dependability and risks in CIs. We reckon that a plausible reason for this may be due to the early and more wide emphasis on these attributes. Another may be attributed to the ease in defining and evaluating the above attributes compared to evaluating resilience. For example, studies [62] indicate a common acknowledgement by power company executives about a better comparative convenience for the ease of defining and

measuring of CI reliability than CI resilience. Be as it may, this acclaimed intractable derivative is now keenly relevant to meet the evolving protection needs of CI sectors.

Understanding and measuring the ability of a system or infrastructure to absorb, adapt and withstand a negative disturbance and rapidly recover back to its initial normal state should be treated as important as understanding and measuring the system's ability to perform what it is intended and expected by design. This is necessary for an efficient CIP implementation plan regardless of the challenges that may be inherent the process. Resilience evaluations would typically depend on the context and dimension within which a study, analysis or modelling is carried out. It would be interesting to explore and see how resilience assessment frameworks [58] integrate with CIP approaches to improve the protective capacities of critical infrastructures.

Evidently, resilience modelling is connected to (inter)dependency. (Inter)dependency analysis contributes information and insights about the degree of impact inducible by failures or disruptions. It also contributes to the perception of the degree of resilience achievable in principle and practice. While some of the CIP approaches acknowledge and consider dependency or cross-dependency relationship and attributes, a larger number of the CIP approaches either implicitly consider it or utterly overlook it. In this era of advancing technology convergence and system hyper-connectivity, understanding the (inter)dependencies amongst CI components and systems can greatly make the difference between ignorance and knowing the nature, type, and degree of resilience required to enhance protection of CIs.

A significant number of the CIP approaches reviewed emerge as instruments delivered by either directly government agencies endowed with protecting CIs, or by research laboratories such as Idaho National Laboratory and Argonne National laboratories also funded by the government. While this presents a good approach towards pushing for wide acceptance of CIP approaches, it is often unclear or in question the extent to which the government-pioneered approaches are practically used in the private sector since most of the CI systems are considerably run by this group. For example, seamless monitoring and reporting of cyber security vulnerabilities and incidents is an aspect which has received reserved attentions and mixed reactions in the private sector and globally in terms of acceptance. Even in cases where mutual cooperation and assistance may significantly support attaining acceptable protection of CIs from threats and attacks, decisions and actions are often determined by growing pressures for competitive advantage [64]. Some of these pressures include: the pressure to; meet global market needs and demands, outdo competitors, protect proprietary information and trade secrets, preserve reputation, manage corporate risks, and limit legal liabilities [65]. Consequently, these more highly regarded business-oriented goals are pursued at the expense of a coordinated and consolidated cybersecurity and protection approach which can be enabled from a shared and collaborative information capability between public (government) and private sector stakeholders. This would have been made available to all players in the CI community.

### 5.2.2 Recommendations

The following recommendations are presented based on the findings of the study:

i. Future improvements and developments in security modelling for critical infrastructure should explore merging two or more existing modelling techniques (especially the most common ones) to leverage on the strengths of the combinations to achieve better results. Consideration should also be given to the capability complements contributed by each technique.

ii. Improvements and future developments in CIP approaches should also focus on addressing latter stages of security risk management, including; management implementation of risks (comprising risk prioritisation and control implementation), and measurement of effectiveness while considering the identification and assessment stages. This can help ensure that a broader and more inclusive scope of security modelling and management is considered and addressed. It will also provide a balanced outlook and response approach to the management of security risks in CI sectors.

iii. Experts and stakeholders within security less-responsive and low interest critical infrastructure sectors such as emergency services, food and agriculture, and dams must draw lessons from the energy and transport sectors. The low interest sectors need to increase and broaden their projections and engagements on the need to adequately protect their systems using very specific and tailored approaches.

iv. Newer CIP modelling approaches should explore continuous/dynamic risk assessment methods [42], [61]. Where possible, CIP modelling and simulation approaches that adopt risk assessment should employ dynamic techniques that can address the security risks as they occur in response to any dynamics or constantly changing CI system components or architecture.

v. CIP modelling approaches need to consider and resilience measures from either structural (topology setup of systems), performance (system performance measure of pre and post disruption) or hybrid (combined structural and performance) approaches. Aside from these static and dynamic factors, economic and human-related factors are also required [58], [63]. Incorporating resilience attributes and evaluation in CIP risk management approaches can significantly support the decision-making process associated with quantifying the effectiveness of preparedness, mitigation, response, recovery and adaptability activities and investments. This can improve the behavioural responses of CIs to disturbance or disruptions.

vi. A strong public-private sector partnership remains invaluable and should be vigorously pursued by both stakeholder groups to achieve better security and resilience (preparation, reaction, and response) in CIs. Such collaboration can enable the public sector to timely and efficiently monitor and aggregate information about CI security risks (threats, vulnerabilities, attack likelihoods, incidents and impacts) as they emerge. They can also provide such information to CI operators (including private sectors) to help them ensure an informed and well-organised security response and management. The effectiveness of security responses and management actions on CI can be influenced by the level of systematic and multidirectional exchange of security risk information between public and private sectors.

### 5.3 Conclusion

There is a reasonable record on the developments and adoption of approaches for engaging or exploring the modelling and simulating critical 'national' infrastructure protection given the invaluable contribution these ventures can bring to a nation's economic stability, growth and development. Going by the outcomes of this study, it is apparent that the task of protecting critical infrastructures is one not to be taken lightly. The number of available security approaches adopted as tools, techniques, methodologies or frameworks related to critical infrastructures is considerably large, and only a sample has been captured in this report.

There is not one CIP approach – a tool, technique, methodology or framework that exists as a 'fit-for-all'. No approach is found to inclusively address holistic modelling and simulation of cyber security risks, resilience, and dependency in all critical infrastructure set-ups. Although some approaches appear to considerably encapsulate a wider scope/stages of security risk management, these approaches often come-off as working methodologies without the complement of software-based systems. Software-based capabilities can help simplify and speed-up security modelling and management processes. Interdependency and resilience modelling, multi-approach integrations, dynamic risk assessment/management, and policy-driven security risk management can all contribute to an improved security risk modelling, simulation and management for critical infrastructure sectors. These factors need to be considered in the selection and adoption of critical infrastructure protection modelling tools and techniques.

In addition, available details about reviewed CIP tools are quite limited as most of the approaches in this category appear to be built and used in-house. There is hardly sufficient information in the public domain on how most of these approaches are used or the outcomes of applying them, such that can provide very clear information and confidence about their usability and effectiveness. To address this, a more coordinated and consolidated security and protection approach for critical infrastructures can be explored via collaborative information sharing between government and private sectors stakeholders. This can support timely and efficient awareness, modelling and evaluation, as well as response to critical infrastructure security risks.

## References


[1] The Council of the European Union, "Council Directive 2008/114/EC of 8 December 2008 on the indentification and designation of European critical infrastructures and the assessment of the need to improve their protection," *Off. J. Eur. Union*, pp. 75–82, 2008.

[2] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, vol. 39, no. 10, pp. 6100–6119, 2011.

[3] S. Croope and S. McNeil, "Improving Resilience of Critical Infrastructure Systems Postdisaster," *Transp. Res. Rec. J. Transp. Res. Board*, vol. 2234, pp. 3–13, 2011.

[4] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 16–23, 2015.

[5] Department of Homeland Security, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," 2013.

[6] C. Pursiainen, "Critical infrastructure resilience: A Nordic model in the making?," *Int. J. Disaster Risk Reduct.*, vol. 27, no. 653390, pp. 632–641, 2018.

[7] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015.

[8] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017.

[9] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016.

[10] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.," European Union, Luxembourg, 2012.

[11] E. Wiseman, "Critical Infrastructure Protection and Resilience Literature Survey: Modeling and Simulation," Ottawa, Canada, 2014.

[12] G. Stergiopoulos, E. Vasilellis, G. Lykou, P. Kotzanikolaou, and D. Gritzalis, "Critical Infrastructure Protection Tools: Classification and Comparison," in *Critical Infrastructure Protection X. ICCIP 2016. IFIP Advances in Information and Communication Technology*, Vol 485., M. Rice and S. Shenoi, Eds. Springer Cham, 2016, pp. 1–25.

[13] CPNI, "Critical National Infrastructure | CPNI | Public Website," *CPNI*, 2018. [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0. [Accessed: 03-Apr-2018].

[14] W. Harrop and A. Matteson, “Cyber resilience: a review of critical national infrastructure and cyber security protection measures applied in the UK and USA.,” *J. Bus. Contin. Emer. Plan.*, vol. 7, no. 2, pp. 149–62, 2013.
[15] P. Sieńko, “Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies in leading,” *Securitologia*, vol. 22, no. 2, pp. 107–123, 2015.
[16] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 43–60, 2014.
[17] E. Bonabeau, “Agent-based modeling: methods and techniques for simulating human systems.,” *Proc. Natl. Acad. Sci.*, vol. 99, no. suppl. 3, pp. 7280–7287, 2002.
[18] E. Casalicchio, E. Galli, S. Tucci, and R. Tor, “Macro and Micro Agent-based Modeling and Simulation of Critical Infrastructures,” in *Complexity in Engineering*, 2010, pp. 79–81.
[19] T. Brown, W. Beyeler, and D. Barton, “Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems,” *Int. J. Crit. Infrastructures*, vol. 1, no. 1, 2004.
[20] S. Armenia, C. Carlini, A. Cardazzone, P. Assogna, E. Brein, and C. D’Alessandro, “A System Dynamics approach to Critical Infrastructures Interdependency Analysis: the experience of the CRISADMIN Project,” in *Proceedings of the 27th International Conference of the System Dynamics Society*, 2009, vol. 1–30.
[21] G. P. O’Reilly, A. Jrad, A. Kelic, and R. Leclaire, “Telecom critical infrastructure simulations: Discrete event simulation vs. dynamic simulation how do they compare?,” in *GLOBECOM - IEEE Global Telecommunications Conference*, 2007, pp. 2597–2601.
[22] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, and D. Reed, “Empirical Framework for Characterizing Infrastructure Failure Interdependencies,” *J. Infrastruct. Syst.*, vol. 13, no. 3, pp. 175–184, 2007.
[23] G. H. Kjølle, I. B. Utne, and O. Gjerde, “Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies,” *Reliab. Eng. Syst. Saf.*, vol. 105, pp. 80–89, 2012.
[24] L. Franchina, M. Carbonelli, L. Gratta, M. Crisci, and D. Perucchini, “An impact-based approach for the analysis of cascading effects in critical infrastructures 2011; 7(1):73-90,” *Int. J. Crit. Infrastructures*, vol. 7, no. 1, pp. 73–90, 2011.
[25] I. B. Utne, P. Hokstad, and J. Vatn, “A method for risk modeling of interdependencies in critical infrastructures,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 6, pp. 671–678, 2011.
[26] B. C. Ezell, J. V. Farr, and I. Wiese, “Infrastructure Risk Analysis Model,” *J. Infrastruct. Syst.*, vol. 6, no. 3, 2000.
[27] B. C. Ezell, J. V. Farr, and I. Wies, “Infrastructure Risk Analysis of Municipal Water Distribution System,” *J. Infrastruct. Syst.*, vol. 6, no. 3, 2000.
[28] J. V. Milanovic and W. Zhu, “Modelling of Interconnected Critical Infrastructure Systems Using Complex Network Theory,” *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–1, 2017.
[29] R. Albert, H. Jeong, and A.-L. Barabasi, “Error and attack tolerance of complex networks,” *Nature*, vol. 409, no. 6819, pp. 542–542, 2001.
[30] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, “Resilience of the Internet to random breakdowns,” *Phys. Rev. Lett.*, vol. 85, no. 21, pp. 4626–4628, 2000.
[31] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, “Breakdown of the Internet under intentional attack,” *Phys. Rev. Lett.*, vol. 87, no. 21, pp. 3682–3685, 2001.
[32] S. V Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.
[33] A. A. Ghorbani and E. Bagheri, “The state of the art in critical infrastructure protection: a framework for convergence,” *Int. J. Crit. Infrastructures*, vol. 4, no. 3, 2008.
[34] E. Cagno, M. De Ambroggi, O. Grande, and P. Trucco, “Risk analysis of underground infrastructures in urban areas,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 1, pp. 139–148, 2011.
[35] Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian, and Z. Yan, “Risk analysis in interdependent infrastructures,” in *IFIP International Federation for Information Processing*, vol. 253, C. Palmer and S. Shenoi, Eds. Springer Berlin Heidelberg, 2007, pp. 297–310.
[36] S. Puuska, K. Kansanen, L. Rummukainen, and J. Vankka, “Modelling and real-time analysis of critical infrastructure using discrete event systems on graphs,” in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2015, pp. 1–5.
[37] L. Crociani, G. Lämmel, H. J. Park, and G. Vizzari, “Cellular Automaton Based Simulation of Large Pedestrian Facilities - A Case Study on the Staten Island Ferry Terminals,” 2017.
[38] Y. Y. Haimes, “Hierarchical Holographic Modeling,” *IEEE Trans. Syst. Man Cybern.*, vol. 11, no. 9, pp. 606–617, 1981.
[39] Y. Y. Haimes, J. Lambert, D. Li, R. Schooff, and V. Tulsani, “Hierarchical holographic modeling for risk identification incomplex systems,” in *1995 IEEE International Conference on Systems, Man and Cybernetics*, 1995, vol. 2, pp. 606–617.
[40] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security - NIST.SP.800-82r2,” 2015.

[41] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, “Taxonomy of information security risk assessment (ISRA),” *Comput. Secur.*, vol. 57, pp. 14–30, 2016.
[42] J. R. C. Nurse, S. Creese, and D. De Roure, “Security Risk Assessment in Internet of Things Systems,” *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.
[43] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate,” *J. Cybersecurity*, vol. 0, no. 0, pp. 1–15, 2018.
[44] G. Amélie, B. Aurélia, and L. Emmanuel, “The Challenge of Critical Infrastructure Dependency Modelling and Simulation for Emergency Management and Decision Making by the Civil Security Authorities.,” in *Critical Information Infrastructures Security. CRITIS 2015. Lecture Notes in Computer Science*, vol. 9578, E. Rome, M. Theocharidou, and S. Wolthusen, Eds. Cham: Springer Cham, 2016, pp. 255–258.
[45] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, “Cascading Effects of Common-Cause Failures in Critical Infrastructures,” in *Critical Infrastructure Protection VII*, Series Vol., vol. 417, no. 2003, J. Butts and S. Shenoi, Eds. Berlin Heidelberg: Springer Berlin Heidelberg, 2013, pp. 171–182.
[46] A. Laugé, J. Hernantes, and J. M. Sarriegi, “Disaster impact assessment:A holistic framework,” in *ISCRAM 2013 Conference Proceedings - 10th International Conference on Information Systems for Crisis Response and Management*, 2013, no. May, pp. 730–734.
[47] R. Setola, E. Luiijf, and M. Theocharidou, “Critical Infrastructures, Protection and Resilience,” Springer Cham, 2016.
[48] R. E. Bloomfield, P. Popov, K. Salako, V. Stankovic, and D. Wright, “Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment,” *Reliab. Eng. Syst. Saf.*, vol. 167, no. March, pp. 198–217, 2017.
[49] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, “Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research,” 2006.
[50] M. Schläpfer, T. Kessler, and W. Kröger, “Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach.” Cornell University Library, pp. 1–8, 2012.
[51] R. Bloomfield, L. Buzna, P. Popov, K. Salako, and D. Wright, *Stochastic modelling of the effects of interdependencies between critical infrastructure*, vol. 6027 LNCS. Springer Berlin Heidelberg, 2010.
[52] R. Bloomfield, N. Chozos, and P. Nobles, “Infrastructure interdependency analysis : Introductory research review,” 2009.
[53] U.S.-Canada Power System Outage Task Force, “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” 2004.
[54] Buncefield Major Incident Investigation Board (BMIIB), “The Buncefield Incident 11 December 2005, Volume 2,” 2008.
[55] U. P. D. Ani, H. (Mary) He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017.
[56] T. Simon, “Critical Infrastructure and the Internet of Things,” Ontario-Canada, 46, 2017.
[57] Australian Government, *Critical Infrastructure Resilience Strategy*, no. September 2001. Commonwealth of Australia, 2010.
[58] A. Alsubaie, K. Alutaibi, and J. Marti, “Resilience Assessment of Interdependent Critical Infrastructure,” *Crit. Inf. Infrastructures Secur. CRITIS 2015. Lect. Notes Comput. Sci.*, vol. 9578, pp. 43–55, 2016.
[59] H. M. A. Rahman, “Modelling and Simulation of Interdependencies between the Communication and Information Technology Infrastructure and other Critical Infrastructures,” Vancouver, BC, Canada, 2009.
[60] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
[61] J. R. C. Nurse, P. Radanliev, S. Creese, and D. De Roure, “If you can’t understand it, you can’t properly assess it! The reality of assessing security risks in Internet of Things systems,” in *2018 IET Conference on Living in the Internet of Things: Cybersecurity of the IoT*, 2018, pp. 1–9.
[62] A. R. Berkeley and M. Wallace, “A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations,” 2010.
[63] A. M. Madni and S. Jackson, “Towards a conceptual framework for resilience engineering,” *IEEE Syst. J.*, vol. 3, no. 2, pp. 181–191, 2009.
[64] J. Perkins, J. Hyde, and A. Falconer, “Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector,” Oxfordshire, 2009.
[65] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection.” European Commission, Brussels, pp. 1–12, 2009.

## Appendix A: Summary description and characterization of critical infrastructure Approaches (Tools and Techniques)

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| ACT | Attack Countermeasure Tree | Tool for developing attack scenarios, identification and selection of best countermeasures. | https://ieeexplore.ieee.org/document/5466633/ | | | |
| ActivitySim | Activity Simulator | Used for modelling the activity representation of US population | http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-08-07134 | | | |
| ADVISE | Adversary-Driven State-based System Security Evaluation | Tool for simulating attacks on systems, and evaluating the probability of attack success. | https://www.perform.illinois.edu/Papers/USAN_papers/10VAN02.pdf | | | |
| AIMS | Agent-based Infrastructure Modelling and Simulation) | Used for analysing the behaviour of interdependent critical infrastructure systems | http://ebagheri.athabascau.ca/papers/ijbpim.pdf | | ■ | |
| AIMSUN | Advanced Interactive Microscopic Simulator for Ur-ban and Non-Urban Networks | Used for Traffic Modelling and Simulation | https://www.aimsun.com/aimsun-next/ | | | |
| AMTI Loki Toolkit | Advanced Modelling & Techniques Investigation (Loki Toolkit | Used for modelling and studies of complex adaptive system of systems related to critical infrastructure interdependencies | http://prod.sandia.gov/techlib/access-control.cgi/2012/121117.pdf | | ■ | |
| AT/FP | Anti-Terrorism/Force Protection | Modelling and planning the perimeter and waterway security of ships in ports | https://savage.nps.edu/RobotTelemetry/DonCioXmlWgNpsSlides/NPSATFPProjectFlyer.2007Apr19.pdf | | | |
| ATAV-SCADA | Attack Trees for Accessing Vulnerabilities in SCADA (Canada) | Tool for calculating the characteristics of the highest attack event | https://www.semanticscholar.org/paper/The-Use-of-Attack-Trees-in-Assessing-in-SCADA-Byres-Franz/02fa72c0bfd76c731201156f81c40952b9da80d1 | | | |
| Athena | - | Used for modelling, identifying and ranking most dependent components/nodes, component/infrastructure vulnerability analysis, direct , cumulative and cascading impacts of changes to infrastructure systems. It also identifies cascading, cumulative, direct and indirect effects on nodes. Used for developing dependency and consequence | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5067457 | | ■ | ■ |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| | | reasoning support to the critical infrastructure (transportation) architecture. | | | | |
| ATOM | Air Transportation Optimization Model | Used for modelling and evaluating the consequences of partial or total outage at an airport or set of airports for a prolonged period of time. | https://books.google.co.uk/books?id=YtXvAgAAQBAJ&pg=PA32&lpg=PA32&dq=Air+Transport+Optimisation+Model+-+ATOM&source=bl&ots=JGVn-y2lvK&sig=3dEXuQBYKh-FrstfbM_wygvNJ_4&hl=en&sa=X&ved=2ahUKEwio57WJnabcAhWQxIUKHZXdCkoQ6AEwB3oECAIQAQ#v=onepage&q=Air%20Transport%20Optimisation%20Model%20-%20ATOM&f=false | | | |
| BIRR | Better Infrastructure Risk and Resilience | Used for assessing vulnerabilities and reporting of risks | http://www.dis.anl.gov/projects/ri.html | ■ | | |
| BLDMP | Boolean Logic Driven Markov Processes | Tool for modelling attacks, characterizing and quantifying potential sequences and steps for attacks. | https://www.sciencedirect.com/science/article/pii/S0951832017301850 | | | |
| BMI | Protection of Critical Infrastructures – Baseline Protection Concept (German Government) | A Methodical plan for risk identification, assessment and control in critical infrastructure domains through cooperation between public and private infrastructure operators. | https://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf | | | |
| CAPRA | Comprehensive Approach for Probabilistic Risk Assessment | Used for modelling, assessing and reporting disaster risk from a probabilistic point of view | https://www.ecapra.org | | | |
| CARVER2 | Criticality Accessibility Recoverability Vulnerability Espyability Redundancy | Used for modelling and prioritization of threats and terrorist targets | http://publications.jrc.ec.europa.eu/repository/bitstream/JRC70046/lbna25286enn.pdf | | | |
| CASCADE | | Used for modelling and analysis of cascading disruptions and failures in large and interconnected infrastructures | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1385362 | | ■ | |
| CEEESA | Centre for energy, environmental, and economic systems analysis (Argonne National Laboratories) | Tools for analyzing network vulnerabilities, modelling gas flows and infrastructure losses | https://ceeesa.es.anl.gov | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| CERT Initiatives | CERT group members: Austria - GovCERT Austria, Finland - NCSC-FI, France - CERT-FR, Germany - CERT-Bund, Netherlands - NCSC-NL, United Kingdom - CERT-UK, etc. | Methodologies for adopting and implementing security teams and capabilities for managing and protecting national critical infrastructures | http://www.egc-group.org/contact.html | | | ■ |
| CERT/CSIRT | Computer (emergency) security incident response team (Carnegie Mellon University) | Tool for monitoring, identification, and prevention of computer security and related incidents | https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf | | | |
| CI3 | Critical Infrastructure Interdependencies Integrator | Used for modelling and estimating the time and costs for partial or complete restoration of critical infrastructures after disruptions or failures. | http://www.ipd.anl.gov/anlpubs/2002/03/42598.pdf | | ■ | |
| CIDA | Critical Infrastructure Dependency Analysis tool | Used for modelling and analysis of the dynamics of cascading failures with time. Also used to model and analyze interdependencies and risk reductions | https://github.com/geostergiop/CIDA/wiki | | ■ | |
| CIMS | Critical Infrastructure Modeling System | Analysis of risk and visualization of cascading impacts of operational anomalies. Used for sensitivity analysis, policy, regulations, and response planning. | http://www.dis.anl.gov/projects/ri.html | ■ | ■ | ■ |
| CIMSuite | Critical Infrastructure Modelling Suite | Used for proactive modelling of critical infrastructure targeted disruptions (natural and human-initiated). | http://www4vip.inl.gov/factsheets/docs/cimsuite.pdf | | ■ | |
| CIP/DSS | Critical Infrastructure Protection Decision Support System | Used for comparative modelling and analysis of risk mitigation strategies on individual infrastructures. Uses scenario-based impact analysis results. | http://public.lanl.gov/dp/CIP.html | | | ■ |
| CIPDSS-DM | Critical Infrastructure Protection Decision Support System Decision Model | Used for modelling decision-making under risks and uncertainty conditions | http://www.ipd.anl.gov/anlpubs/2008/12/63060.pdf | | | ■ |
| CIPMA | Critical Infra-structure Protection Modeling and Analysis | Used for evaluating failures, dependencies and resilience of critical infrastructure, as well as cascading impacts on other infrastructures. Supports the development of policies and regulations for national security | http://www.dis.anl.gov/projects/ri.html | ■ | ■ | ■ |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| CISIA | Critical Infrastructure Simulation by Interdependent Agents | Used for modelling agents/system interdependencies, and analysis of emergency responses and their origin. | http://www.chiarafoglietta.com/wp-content/uploads/2015/04/Cisia.pdf | | ■ | |
| COMM-ASPEN | Agent-based simulation model of the US economy | Used for modelling the effects of market decision and disruptions of telecommunications infrastructure to the economy. | http://www.dis.anl.gov/projects/ri.html | | ■ | |
| CORAS-BRA-SCADA | CORAS-Based Risk Assessment for SCADA (USA). | Tool for modelling the risks of ICS prototypes using the CORAS framework | https://pdfs.semanticscholar.org/3143/940955a76a49646ba2954e0735a0ec18d7ca.pdf | | | |
| COUNTERACT | Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities | Used for risk assessment, mitigation and reporting | http://www.dis.anl.gov/projects/ri.html | | | |
| CSASG-SCADA Systems with Game Models | Cyber Security Analysis of Smart Grid SCADA Information Security (USA) | Tool for identifying the best action strategy for attackers and defenders, and relative payoffs. | https://dl.acm.org/citation.cfm?id=2602089 | | | |
| CSRA-NPP | Cyber Security Risk Assessment in Nuclear Power Plants (Korea) | Tool for identifying and characterizing risk assessment activities at initial design stages | http://koreascience.or.kr/article/ArticleFullRecord.jsp?cn=OJRHBJ_2012_v44n8_919 | | | |
| Cy-T SCADA RF | Cyber-Terrorism SCADA Risk Framework (Australia) | Measuring cyber-terrorism threats and implementing control measures | http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=isw | | | |
| DECRIS | Risk and Decision Systems for Critical Infrastructures | Used for risk and vulnerability analyses that focus on critical infrastructure (drinking water, energy supply, transportation, ICT) interdependencies. | https://www.sintef.no/projectweb/samrisk/decris/ | ■ | | |
| DEW | Distributed engineering workstation (Electrical Distribution Design, Inc. Sponsored by DOE and DoD) | Tool for identification and analysis of interdependencies, asset management, and operations planning for power systems. | https://www.eee.hku.hk/~cees/software/dew.htm | | ■ | |
| DMRIM-SCADA System | Digraph Model for Risk Identification and Management in SCADA System (USA). | Tool for vulnerability identification, faults and failure diagnosis, and risk impact assessment. | https://ieeexplore.ieee.org/document/5983990/ | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| DUTCH NRA | Dutch Government | Tool used for analyzing threats and hazards using multi-criteria decision making techniques to achieve reduction of risks. | https://english.nctv.nl/binaries/poster-st-geneva-2015-analyst-network-(8)_tcm32-84227.pdf | ■ | | ■ |
| EAR-PILAR | National Cryptology Centre Spain | A tool for asset characterization, risk (threats, vulnerabilities, and impacts) modelling, and control evaluations. Considers identification, classification, ratings, and dependencies amongst assets | http://www.pilar-tools.com/en/tools/pilar/v71/index.html | | ■ | ■ |
| ECI-GIS | Geographic information systems and risk assessment (EU sponsored Joint Research Centre). | A tool for modelling operational continuity following loss and damage of critical infrastructures. | https://core.ac.uk/download/pdf/38613171.pdf | | | |
| EMCAS | Electricity Market Complex Adaptive System | Used for modelling and evaluating operational and economic impacts of various external events on complex power systems (e.g. electricity) | https://www.energyplan.eu/othertools/national/emcas/ | | | |
| EpiSimS | Epidemic Simulations | Used for modeling and analysis of the spread of diseases | http://public.lanl.gov/sdelvall/p556-mniszewski.pdf | | | |
| EPRAM | Electric Restoration Analysis Tools | Used for modelling electric power restoration | http://www.mssanz.org.au/modsim2013/D2/stamber.pdf | | | |
| ERC-SCADA System-Petri Net Analysis | Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis. | Tool for evaluating operational risks using non-probabilistic metrics approach. | https://ieeexplore.ieee.org/document/5168093/ | | | |
| EURACOM | European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks | All-hazard risk assessment and contingency scheduling. | http://www.dis.anl.gov/projects/ri.html | ■ | | |
| FAIT | Fast Analysis Infrastructure Tool (Sandia National Lab, sponsored by US DHS) | Knowledge base tool (including emergency network and georeferencing data) for performing economic impact analysis across multiple critical infrastructure sectors. | http://www.dis.anl.gov/projects/ri.html | ■ | | |
| FastTrans | Los Alamos National Lab | A parallel microsimulator tool for transportation networks for simulating and routing very large numbers of vehicles on real-world road networks in a fraction of real time. | https://www.lanl.gov/orgs/adtsc/publications/science_highlights_2011/docs/6InfoSciPDFs/sunil.pdf | | | |
| FEPVA | Framework for Electricity Production Vulnerability | Tool for assessing the potential impact of natural disasters or malicious attacks for both response and preventative | https://www.gpo.gov/fdsys/pkg/GOVPUB-C13- | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| | Assessment (Los Alamos National Lab) | purposes. Specifically used to determine the power plants with impact potentials and the extent feasible. | f3de19ca7b535ba3207a5be512241f84/pdf/GOVPUB-C13-f3de19ca7b535ba3207a5be512241f84.pdf | | | |
| FINSIM | Financial System Infrastructure (Los Alamos National Lab) | Tool for modelling financial service sector as a complex decentralized system with multiple interacting autonomous decision nodes or agents such as banks, traders, markets, and brokers. | https://cnls.lanl.gov/annual26/abstracts.html | | | |
| FMEA/FMECA | Failure Mode Effect and Criticality analysis | Technique for analyzing probable system failures, enumerating potential impacts, and classifying control and mitigation actions. | https://pdfs.semanticscholar.org/aba3/1bf32898f29ea56be2e1f5b4f99938face35.pdf | | | |
| Fort Future | US Army Corps of Engineers | A tool that follows a multiple simulation approach for multi-criteria decision support. Used for simulating test plans for Department of Defense installations, and evaluating a set of alternatives. | https://ascelibrary.org/doi/pdf/10.1061/40794%28179%2922 | ■ | | ■ |
| FTA | Fault Tree Analysis | A deductive technique for evaluating risk causes from a combination of inputs. | http://asq.org/quality-progress/2002/03/problem-solving/what-is-a-fault-tree-analysis.html | | | |
| GAMS-CERO ERA | Enterprise Risk Assessment | Technique for managing and mitigating risk using administrative procedures and resources. | | | | ■ |
| GIS Interoperability | Geographical Information Systems Interoperability | A methodology for emergency coordination and support using geographical information systems. | https://books.google.co.uk/books?id=eoB6nTkhLqkC&pg=PA388&lpg=PA388&dq=Challenges+for+the+application+of+GIS+interoperability+in+emergency+management&source=bl&ots=A9AYBmqk0n&sig=EaYUOn_X24FOalYX3rXlAvFVyuw&hl=en&sa=X&ved=2ahUKEwjRqIHz67XdAhUHLewKHTCiBo0Q6AEwAHoECAAQAQ#v=onepage&q=Challenges%20for%20the%20application%20of%20GIS%20interoperability%20in%20emergency%20management&f=false | | | |
| GoRAF | University of New Brunswick (Canada) | A tool for critical infrastructure resource identification, and metric-based estimation of economic losses. | https://www.inderscienceonline.com/doi/pdf/10.1504/IJRAM.2007.015297 | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| HAZOP | Hazard and Operability Analysis | Technique for system examination and risk management based on theory of assumptions that risk events occur due to deviations from design and operating plans. | http://pqri.org/wp-content/uploads/2015/08/pdf/HAZOP_Training_Guide.pdf | ■ | | ■ |
| HCSim | Healthcare Simulation (Los Alamos National Lab) | A modelling tool for assessing the impact of mass casualties in health care and public health institutions (e.g., hospitals) | https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-13-24605 | | | |
| HM-BRMCI | Hierarchical, model-based risk Management of Critical Infrastructures | Tool for automating the definition of risk mitigation plans and activities. | https://www.sciencedirect.com/science/article/pii/S0951832009000349 | | ■ | |
| HURT | Hurricane Re-location Tool (Los Alamos National Lab) | A tool for modelling the relocation of Hurricane | http://www.lanl.gov | | | |
| HYDRA Pop & Eco Modeling | (Los Alamos National Lab) | Integrated service-oriented architevture tool for modeling and simulating infrastructures with seamless interoperability. | https://public.lanl.gov/rbent/hydra-with-cover.pdf | | | |
| I2SIM | Infrastructures Interdependencies Simulation (University of British Columbia) | A tool for simulating scenarios for disaster responses at system level with impact characterization. | http://www.ece.ubc.ca/%7Ejiirp/ | | ■ | |
| ICS-CDTP | Industrial Control System Cyber Defense Triage Process | Tool for threat analysis, attack modelling, and control and countermeasure applications | https://www.sciencedirect.com/science/article/pii/S0167404817301505 | | | |
| IEISS | Interdependent Environment for Infra-structure System Simulations (University of Virginia) | A modelling tool for simulating electricity and natural gas flow, outage characteristics, and system interdependencies. | http://www.bwbush.io/projects/ieiss.html | | ■ | ■ |
| IIM | Inoperability In-put-Output Model (Sandia National Labs and Los Alamos National Labs) | A tool for sector-based economic impact analysis of infrastructure attacks and failures. | https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%291076-0342%282005%2911%3A2%2867%29 | ■ | ■ | ■ |
| Infrastructure Disruptions | - | Tool for modelling the state of infrastructure systems under abnormal conditions, and evaluating the economic consequences of abnormalities. | | | | ■ |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| INTEPOINT VU | IntePoint LLC | A modelling tool that combines various techniques for complex environments analysis and system-wide interdependencies modelling across physical, virtual and social networks. | https://www.nist.gov/sites/default/files/documents/el/msid/Critical_Infrastructure.pdf | | ■ | |
| IRAM | Infrastructure risk analysis model (US Military Academy) | Tool used to model and simulate resource allocation for interconnected infrastructure reliability. Used for risk quantification. | https://ascelibrary.org/doi/10.1061/%28ASCE%291076-0342%282000%296%3A3%28114%29 | | | |
| IRAM-SCADA INFORMATION Sec | Improved Risk Assessment Method for SCADA Information Security (Serbia) | Evaluating the effectiveness of intrusion, detection, and prevention systems in controlling attacks. | http://eejournal.ktu.lt/index.php/elt/article/view/8027/4033 | | | |
| IRRIIS | Integrated Risk Reduction of In-formation-based Infra-structure Systems (IRRIIS Project, EU) | Interdependency and resilience modelling, analysis and management of critical infrastructures | https://www.irriis.org | ■ | ■ | |
| Knowledge Mgt & Visualisation | Carnegie Mellon University | Tool for analyzing vulnerabilities related to the distribution of fuel | https://inldigitallibrary.inl.gov/sti/3489532.pdf | | | ■ |
| LogiSims | Los Alamos National Laboratory | Tool for modelling and planning preparation for a disasters and concurrent responses to a disaster | http://public.lanl.gov/rbent/bent-pes.pdf | ■ | | |
| LS-DYNA | Livermore Software Technology Corporation | A tool for modelling large complex system structures and behaviours related to failures such as: changing boundary conditions, deformations, crashes and explosions. | http://www.lstc.com/products/ls-dyna | | | |
| LUND | University of Lund (Sweden). Sponsored by the International Energy Agency | Grounded Network theory methodology for modelling the relationships between nodes in a system of roads or rail interconnected transport infrastructure. | https://www.iea.lth.se/publications/Theses/LTH-IEA-1061.pdf | | ■ | |
| MARGERIT V2 | Spanish Ministry for Public Administrations | methodology for Risk Analysis and Management for security of computer systems, digital and data networks. | https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html | | | ■ |
| MBRA | Model-Based Risk Assessment (Naval Postgraduate School, Center for Homeland Defense & Security) | Analysis of critical infrastructure network components and faults for efficient resource allocation | https://www.chds.us/ed/items/2164 | ■ | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| MIA | Methodology for Interdependency Assessment | A methodology for identifying and characterizing critical interdependencies of the systems in relations security vulnerabilities. | https://link.springer.com/content/pdf/10.1007%2F978-3-642-21694-7_1.pdf | | ■ | ■ |
| MIITS | Multi-Scale Integrated Information & Telecommunications System (Los Alamos National Laboratories) | A tool for simulating high fidelity network topology, internet communication sessions and packets, and actual scalability representations. | https://ieeexplore.ieee.org/document/4117861/ | | | |
| MIN | Multi-layer Infrastructure Networks (Purdue University) | A simulation tool for solving flow equilibrium and optimal budget allocation problem related to automobile, urban freight and data network layer | https://link.springer.com/content/pdf/10.1007%2Fs11067-005-2627-0.pdf | | | |
| Modular Dynamic Model | Sandia National Laboratory | A tool for modelling and simulating energy infrastructure interdependency operations including generation, transmission, distributions and trading. | https://www.sandia.gov/nisac-ssl/wp/wp-content/uploads/downloads/2012/04/a-modular-dynamic-simulation-model.pdf | | | |
| MSM | MIT Screening Methodology (MIT = Massachusetts Institute of Technology) | A methodology for prioritizing vulnerabilities | | | | |
| MUNICIPAL | Multi-Network Interdependent Critical Infrastructure Program for Analysis of Lifelines (Rensselaer Poly-technic Institute, USA) | A decision support tool simulating infrastructure moving parts and interdependencies within coastal regions to define optimal response before, during and after hazards. | http://eaton.math.rpi.edu/faculty/Mitchell/papers/decisiontechnologies.pdf | | ■ | |
| N-ABLE | National A-gent-Based Laboratory for Economics (Sandia National Laboratories and Los Alamos National Laboratories) | A tool for analyzing economic factors, responses and downstream consequences of infrastructure interdependencies | http://www.dis.anl.gov/projects/ri.html | | ■ | ■ |
| NEMO | Net-Centric Effects-based Operations Model (Sparta, Inc.) | A tool for modelling impact cascades of events through multiple infrastructure networks, and determining the results of course of actions. | http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf | | ■ | |
| Neptune Tides | Neptune Navigation Software (UK) | A tool for simulating wind speed and analysis of flood surges. | http://www.neptunenavigation.co.uk/tides.htm | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| Net-Centric GIS | York University | A tool that used to support decision making propositions using GIS interoperability features. | https://inldigitallibrary.inl.gov/sti/3489532.pdf | | | |
| NEXUS Fusion Framework | IntePoint, LLC | A tool for modelling and visualizing planned and unplanned effects and consequences of an event through multiple infrastructures | https://www.oii.ox.ac.uk/research/projects/nexus/ | | ■ | |
| NGAT | Natural Gas Analysis Tools (Argonne National Laboratories) | A tool for modelling natural gas pipeline infrastructures | https://inldigitallibrary.inl.gov/sti/3489532.pdf | | | |
| NGFast | Natural Gas Fast (Argonne National Laboratory) | A tool for simulating natural gas systems, and impact assessment of pipeline breaks or failures. | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4419711 | | | |
| NIPP-RMF | National Infrastructure Protection Plan – Risk Management Framework (Dept. of Homeland Security) | A process methodology for risk management for protecting critical infrastructures. It combines threats, vulnerability and consequence analysis to drive prioritization of effective controls to minimize impacts. | https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf | ■ | | |
| NSRAM | Network Security Risk Assessment Method (James Madison University) | Analysis of cyber and physical infrastructure security risks, determining the response nature of system to attacks and incidents | https://works.bepress.com/george_h_baker/12/download/ | | | |
| NSRM | Network Security Risk Model | Methodology used to support the selection of risk management countermeasures and controls | https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1539-6924.2008.01151.x | | | |
| OGC CIPI | Critical Infrastructure Protection Initiative (Open Geospatial Consortium) | A methodology for managing emergency incidents through inter-agency data exchange and alert notifications | http://www.opengeospatial.org/projects/initiatives/cipi1.2 | | | ■ |
| PCI-Information | Projects of Common Information (Joint Research Centre, Sponsored by the European Commission) | A methodology for standardizing energy communication systems of European Union stakeholders and regulators | https://ec.europa.eu/energy/en/topics/infrastructure/projects-common-interest | | | ■ |
| PFNAM | Petroleum Fuels Network Analysis Model (Argonne National Laboratories) | A tool for hydraulic computation of crude oil and petroleum products transportation via pipelines. | http://www.gss.anl.gov/publications-2/ | | | |
| PipelineNet | US Federal Emergency Management Agency and | A GIS-based tool for modelling the flow and concentration of contaminants in water pipeline infrastructures. Also used to estimate risks to public water supply. | https://www.tswg.gov/sites/default/files/publications/PipelineNet%20TB.pdf | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| | the Environmental Protection Agency | | | | | |
| PMU-Based RAFPCS | PMU-Based Risk Assessment Framework for Power Control Systems (USA) | Tool for real-time monitoring cyber intrusion impacts on the behaviours/dynamics of power systems. | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6672731 | | | |
| QCRREM | Quantitative Cyber Risk Reduction Estimation Methodology (USA) | Tool for evaluating risk reductions in an enhanced security SCADA System. | https://ieeexplore.ieee.org/document/1579754/ | | | |
| QCSRAM-SCADA | Quantitative Cyber Security Risk Assessment Methodology | Tool for assessing vulnerabilities from historic data related to threats, asset value, and outage costs | https://www.scientific.net/AMR.960-961.1602 | | | |
| QMACSR-SCADA Systems | Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems (Korea) | Tool for calculating cyber threats expected damage | https://www.scientific.net/AMR.960-961.1602 | | ■ | |
| QTRIM | Quantitative Threat-Risk Index Model (Idaho National Engineering and Environmental Laboratory) | Tool used for evaluating security risks in relations to terrorist attacks against national infrastructures. | https://inldigitallibrary.inl.gov/sites/sti/sti/2535260.pdf | | | |
| QualNet | Scalable Network Technologies, Inc | A tool for modelling and analysing the behaviour of real communications networks. | https://web.scalable-networks.com/qualnet-network-simulator-software | | | |
| R-NAS | Railroad Net-work Analysis System (Sandia National Laboratories and Los Alamos National Laboratories) | A tool for modelling the impacts to the flow of commodities over the rail network and infrastructure in the US, especially when one or more components of the rail system are unavailable. | https://www.sandia.gov/nisac-ssl/wp/wp-content/uploads/RNAS-20160119_SAND2016-1408M.pdf | | | |
| RA-SCADA Railways | Risk Assessment in GPS-based SCADA for Railways (USA) | Identification of the origin of risks | https://ac.els-cdn.com/S0167404815001388/1-s2.0-S0167404815001388-main.pdf?_tid=dd19f4ca-8664-4262-86fb-3a4c728f32a1&acdnat=1534163806_56cd404652f32b69a028bf6a20a63b3d | | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| RADR | Risk Assessment Detection and Response | Identifying sensors with high priorities for prioritizing security budgets | https://pdfs.semanticscholar.org/ee2e/e3dca15c4836b07c7a0e2c265329a9298901.pdf | | | |
| RAIM | Real-time Monitoring, Anomaly detections, Impact analysis, and Mitigation Strategies SCADA security framework | A tool for real-time monitoring and anomaly detection, impact analysis and security control implementations in power control SCADA infrastructure networks. | https://ieeexplore.ieee.org/document/5477189/ | | | |
| RAMCA | Risk-Assessment Model for Cyber Attacks. | Tool for calculating summed losses on revenue related to cyber-attacks. | https://pdfs.semanticscholar.org/8a41/a48819b6ecf62424bb4d6041a8a31a630cfe.pdf | | | |
| RAMCAP-Plus | Risk Analysis and Management for Critical Asset Protection Plus (American Society of Mechanical Engineers) | A methodology for the assessment of risk and resilience and prioritization across all critical infrastructure sectors | http://files.asme.org/ASMEITI/RAMCAP/17978.pdf | ■ | | |
| Restore | Interdependent Repair and Restoration Processes (Argonne National Laboratories) | A tool for modelling the restoration and recovery of critical infrastructure systems from incidents. Used to estimate time and cost attributes of restoration goals. | http://www.anl.gov/egs/group/resilient-infrastructure/resilient-infrastructure-capabilities | | | |
| Risk Maps | Risk Mapping, Planning and Assessment. | A Methodology for systematic risk inventory management including support planning to reduce risk impacts | https://www.fema.gov/risk-mapping-assessment-and-planning-risk-map | ■ | | ■ |
| RMGCIS | Risk Management Guide for Critical Infrastructure Sectors (Canada) | A methodology for risk and resilience assessment and control implementations. | https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf | ■ | | |
| RTDS | Real Time Digital Simulator (RTDS Technologies Inc) | A tool for real-time simulating and testing the changing behavior of power systems. | https://www.rtds.com | | | |
| RVA | Risk and Vulnerability Analysis (Danish Emergency Management Agency) | A methodology for analyzing threats, vulnerabilities and risks in critical infrastructure sectors. It also supports prioritization for effective vulnerability and risk controls. | http://brs.dk/eng/inspection/contingency_planning/Documents/RVA-model_user_%20guide.pdf | | | |
| S-RAM | Risk Assessment methodology (Sandia National laboratory) | A methodology for automated assessment of risks and resilience related to physical critical infrastructure attacks | https://prod.sandia.gov/techlib-noauth/access-control.cgi/2008/088143.pdf | ■ | | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| SAIV | Security of Activities of Vital Importance (French Government) | Methodology for protection critical infrastructures based on private-public sector discussions, and priority-based support of security across critical infrastructure sectors. | https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/ | | | ■ |
| SC-Based ARAC | Scenario-based Approach to Risk Analysis in Support of Cyber Security (USA) | Used to support effective resource allocation in finances and personnel for critical attacks | https://inis.iaea.org/search/searchsinglerecord.aspx?recordsFor=SingleRecord&RN=43118741 | | | |
| SessionSim | Los Alamos National Laboratories | A tool for generating realistic communication sessions or data traffic | https://ieeexplore.ieee.org/document/5429274/ | | | |
| SIERRA | System for Import/Export Routing and Recovery Analysis (Sandia National Laboratories and Los Alamos National Laboratories) | A tool for modelling and estimating flow diversion between ports. | https://www.osti.gov/servlets/purl/1142053 | | | |
| SRM-ICSP | Security Risk Methodology for Instrumentation and Control System Processes | Tool for assessing cyber risks for nuclear instrumentation and control systems using Bayesian networks and event tree modelling techniques. | https://www.sciencedirect.com/science/article/pii/S1738573316302935 | | | |
| TEVA | Threat Ensemble Vulnerability Assessment (EPA) | A tool for analysing the vulnerabilities of water distribution systems, measuring public health and economic impacts, and modelling threat mitigation and response strategies. | https://ascelibrary.org/doi/abs/10.1061/40737%282004%29482 | | | |
| TIMQAV-CIS | Two Indices Method for Quantitative Assessment of the Vulnerability of Critical Information Systems | Tool use to support informed decisions about countermeasures related to security vulnerabilities. | https://www.sciencedirect.com/science/article/pii/S0268401208000054?via%3Dihub | | ■ | |
| TRAGIS | Transportation Routing Analysis Geographic Information System (Oak Ridge National Laboratories) | A tool for modelling transportation (rail, waterway and highway) routing | https://web.ornl.gov/sci/gist/TRAGIS_2005.pdf | | | ■ |
| TranSims | Transportation Analysis Simulation System (Los Alamos National Laboratories) | A tool for simulating vehicular movements, and analyzing the consequences of urban transportation system. | https://code.google.com/archive/p/transims/ | | | |
| UIS | Urban Infrastructure Suite (Los Alamos National Lab) | A tool for simulating interactive urban infrastructures, their behaviours and effects of interdependencies. | http://www.sandia.gov/nisac/uis.html | | ■ | |

| CIP Approaches | Full Meaning | Purpose Description | Web Link | Resilience | Interdependency | Policy and Regulations |
|---|---|---|---|---|---|---|
| UML-CI | University of New Brunswick, Fredericton, Canada | A reference method for modelling infrastructure systems high-level metamodels to aid system profiling and management. | https://link.springer.com/article/10.1007/s10796-008-9127-y | | | ■ |
| UPMoST | Urban Population Mobility Simulation Technologies (National Infrastructure Simulation and Analysis Center) | A tool used to model the movement of entities across multiple domains and interfaces. | https://ieeexplore.ieee.org/abstract/document/1265180/ | | | |
| USArmy Risk Mitigation | Los Alamos National Laboratory | A tool for simulating the management of fresh water network infrastructure in relations to usage at U.S. military bases. | https://www.systemdynamics.org/assets/conferences/2001/papers/Lee_MA_1.pdf | | | |
| VACSPI | Vulnerability Assessment of Cyber Security in Power Industry | For estimating cyber vulnerability indices of infrastructures in the power sector. | https://ieeexplore.ieee.org/document/4076075/ | | | |
| VAM-SCADA Security | Vulnerability Assessment Methodology for SCADA Security | Tool for assessing vulnerabilities and the security of SCADA system | https://inldigitallibrary.inl.gov/sites/sti/sti/3562811.pdf | | | |
| VINCI | Virtual Interacting network Community (University of Pisa, Italy) | A tool for modelling secure network management architecture for critical infrastructures using virtualization capabilities. | https://ieeexplore.ieee.org/document/5628730/ | | | |
| VISAC | Visual Interactive Site Analysis Code (Oak Ridge National Laboratory) | A tool for analysing accidents/incidents at nuclear or industrial facilities, and modelling the range of damaged and downtime. | https://www.visac.ornl.gov/HelpFiles/iitsec02.html | | | |
| WISE | Water Infrastructure Simulation Environment (Los Alamos National Laboratories) | A tool for infrastructure and interdependency analysis of water and waste water flows. | https://ascelibrary.org/doi/10.1061/40792%28173%2958 | | ■ | |