Doctoral theses at NTNU, 2023:83

Aida Akbarzadeh

Dependency based risk analysis in Cyber-Physical Systems

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of Philosophiae Doctor
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

Aida Akbarzadeh

Dependency based risk analysis in Cyber-Physical Systems

Thesis for the Degree of Philosophiae Doctor

Trondheim, Gjøvik 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

ISBN 978-82-326-6576-1 (printed ver.)
ISBN 978-82-326-6986-8 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2023:83

Printed by NTNU Grafisk senter

To my parents ♡
and you

"The flutter of a butterfly's wing,
Sets off a chain of events unseen,
Our lives are woven, like a string,
With others, in an intricate scheme.

Our fate entwined, in cause and effect,
Our actions have a ripple effect on us,
Better be aware, and take the lead,
To make a difference, in word and deed.

Let us not be afraid to lean on each other,
For in interdependence, there is no other way,
For in the end, we all depend,
On one another, till the very end."

Declaration of Authorship

I, Aida Akbarzadeh, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:
Aida Akbarzadeh

Date: March 2023

Abstract

The term "cyber-physical systems" was introduced by Helen Gill at the National Science Foundation around 2006. Cyber-Physical Systems (CPSs) are systems that integrate computation, communication, and controlling capabilities of Information and Communication Technology (ICT), with the traditional infrastructures. This integration aims to facilitate the monitoring and controlling of objects in the physical world as one of the essential requirements of different Critical Infrastructures (CIs), such as manufacturing, healthcare, transportation, and the energy sector [1]. CPSs can be seen as the forerunners of *'smart'* solutions, such as *smart grids*, and *smart cities*.

By moving towards Industry 4.0, the integration between Information Technology (IT) and Operational Technology (OT) has significantly increased and exacerbated the complexity of CPSs. This hinders the comprehensive understanding of interactions in CPSs and causes many interdependencies. An interdependency in a CPS, which mainly refers to the relationship between the IT and OT parts, implies that a failure in the IT part might impact the functionality of the OT and vice versa. While we are witnessing the growing number of cyber attacks that target IT systems on a daily basis and, as the border between OT and IT is disappearing, CPSs are turning into attractive targets for cyber attacks. Adversaries can take advantage of complex interdependencies in such systems to infiltrate the OT part, affect the operational part of CPSs, and impose safety risks. Indeed, the security of CPSs highly demands a paradigm shift in conventional security methods in particular risk assessment methods. To enhance the security of CPSs and protect them against emerging cyber attacks, an end-to-end mechanism is needed to analyze interactions within the system components to reveal the hidden dependencies as the potential infiltration points across the systems that might be leveraged by adversaries. To this end, this PhD research aims to contribute to improving the security of cyber-physical systems by concentrating on the concept of interdependency and providing a risk assessment method. Interdependency analysis in CPSs is a multifaceted objective that encompasses identification, modeling, and feature extraction in such a way as to support the process of security risk assessment in cyber-physical systems from a unified IT and OT perspective.

The results of this PhD research have been published in three journal articles and three articles in conference proceedings, included in the second part of the thesis.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my main supervisor, Prof. Sokratis Katsikas, for his unwavering support and guidance throughout my Ph.D. journey. I am forever grateful for his encouragement and belief in my abilities which allowed me to challenge myself and step into my growth zone, where I could explore new things and accept new responsibilities. And I would also like to extend my sincere appreciation to my co-supervisors, Katina Kralevska and Pankaj Pandey, for their support.

Furthermore, I would like to thank the committee members for their valuable feedback throughout the process of evaluating my dissertation. Their suggestions have greatly improved this work.

I am grateful for the love and support of my family, friends, and all members of the CISaR group, who have been a constant source of inspiration throughout the ups and downs. This journey has not shaped my research only, but also my perspective on life.

Last but not least, I would like to express my gratitude to all my colleagues in the Faculty of Information Technology and Electrical Engineering, Gjøvik and Trondheim, and everyone who has facilitated working on this research. Their support and guidance have been invaluable, and I am deeply grateful for their role in my journey.

Contents

List of Figures

List of Tables

Abbreviations

ANP Analytic Network Process

BDMP Boolean logic Driven Markov Process

BG Bond Graph

BN Bayesian Network

CN Complex Network

CNN Convolutional Neural Network

CoD Criticality of Dependency

CPS Cyber-Physical Systems

CI Critical Infrastructure

CISA Cybersecurity and Infrastructure Security Agency

CT Graph Theory

CPTL Cyber-Physical Topology Language

DCS Distributed Control Systems

DEMATEL Decision Making Trial and Evaluation Laboratory

DFS Depth-First Search

FACT Failure-Attack-CounTermeasure

FMEA Failure Mode and Effect Analysis

FRAM Functional Resonance Analysis Method

ICA Imperialist Competitive Algorithm

ICS Industrial Control System

ICT Information and Communication Technology

IoD Impact of Dependency

IT Information Technology

MADM Multiple Attribute Decision Making

MDSM Modified Dependency Structure Matrix

M-TOPSIS Modified - Technique for Order Preference by Similarity to Ideal Solution

NIST National Institute for Standards and Technologies

OT Operational Technology

POMDP Partially Observable Markov decision process

SCADA Supervisory Control and Data Acquisition

SGAM Smart Grids Architecture Model

SoD Susceptibility of Dependency

SoS System of Systems

STAMP System Theoretic Accident Model and Processes

TIC Tacit Input Centrality

TOC Tacit Output Centrality

VPN Virtual Private Network

WoD Weight of Dependency

Part I: Overview

1 Introduction and motivation

1.1 Introduction

Traditionally, the worlds of information technology and operational technology have been separated at the technical and organizational levels in different industries, and each of them keeps separate technology stacks and has its specific protocols and standards [16, 17]. However, the advent of Industry 4.0 and the recent trend toward automation and the leveraging of information and communication technology in monitoring and control of CPSs in critical infrastructures, is about to blur this separation and open the doors for integrating IT and OT (see figure 1). Information technology, which implements mainly the *cyber* part, allows the cooperation and communication of technologies for information processing and technologies for monitoring, control, and maintenance purposes. Operational technology mainly implies the *physical* aspects of CPSs and directly interfaces with the physical processes of the systems under the monitor to manage and control the procedures of physical value creation and correction in various equipment.

In the domain of cybersecurity, the National Institute for Standards and Technologies (NIST) defined OT as [10]:

> "Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events."

Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems

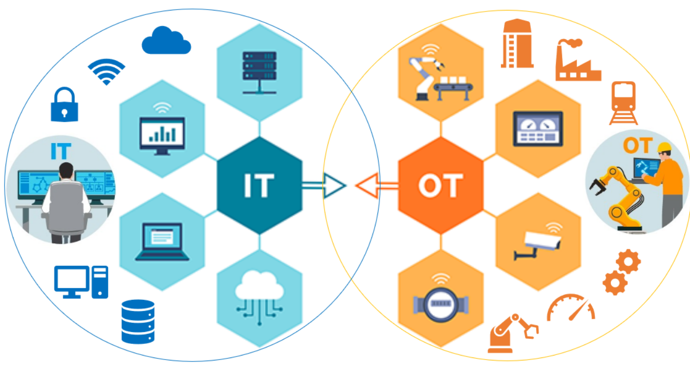


Figure 1: IT-OT convergence.

(DCS) which are widely utilized to monitor and control critical infrastructures are classified as Operational Technology. Accordingly, OT has been applied in different industries and critical infrastructures. The Cybersecurity and Infrastructure Security Agency (CISA) identified the following sectors as critical infrastructures holding OT-based systems [9]:
- Energy Sector
- Critical Manufacturing Sector
- Healthcare and Public Health Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Chemical Sector
- Commercial Facilities Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Nuclear Reactors, Materials, and Waste Sector

The fast progress in the IT domain caused stakeholders to wish to equip critical infrastructures with advanced technologies to enhance the productivity and quality of the processes. As a result, IT capabilities such as networking functionality were gradually inserted into existing physical systems to enable internet connection and provide remote monitoring and control [18]. Yet, OT characteristics, such as their long life cycles, have not changed, and two main paradigms still dominate the OT domain, i.e., "safety comes first", and "if it is working, do not touch it" [17]. The latter is one of the main reasons for using legacy equipment and software in industrial control systems, particularly in the OT part. Therefore, many OT systems are operated with legacy software that cannot appropriately authenticate users and lack data integrity verification capabilities. A recent report released by Microsoft in 2022 revealed that 29 percent of Windows operating systems in OT environments have versions that are no longer supported, such as Windows XP and Windows 2000 [1]. Since availability is crucial in OT systems, communications are typically in plain text, and industrial protocols in SCADA do not always support encryption. Therefore, attackers may utilize sniffing software to listen to messages (passive recognizance), and discover confidential information like usernames and passwords or launch man-in-the-middle attacks [19]. It should be considered that protocols run in OT systems such as Common Industrial Protocol (CIP), Modbus, MTConnect, DNP3, Profinet, and EtherCAT have been built for different purposes, without security in mind. As a result, such protocols are more vulnerable to attacks than IP-based protocols employed in the IT domain. High availability also means software upgrades and patches must be scheduled days/weeks in advance and should usually be done by the corresponding vendors. Microsoft reported that they identified unpatched high-severity vulnerabilities in 75% of the most common industrial controllers in their customers' OT networks. Table 1, adapted from the NIST guide [9], summarizes the typical differences between IT and OT systems.

[1] https://shortest.link/bhfh

Table 1: Comparison between IT and OT systems [9]

IT	OT
Non-real time	Real-time
Response must be consistent.	Response is time-critical.
High throughput is demanded.	Modest throughput is acceptable.
High delay and jitter may be acceptable.	High delay and/or jitter is not acceptable.
Emergency interaction is less critical.	Response to human and other emergency interactions is critical.
Tightly restricted access control can be implemented to the degree necessary for security.	Access to OT should be strictly controlled but should not hamper or interfere with human-machine interaction.
Responses such as rebooting are acceptable.	Responses such as rebooting may not be acceptable because of process availability requirements.
Availability deficiencies can often be tolerated, depending on the system's operational requirements.	High availability requires exhaustive pre-deployment testing and outages must be planned and scheduled days/weeks in advance.
Data confidentiality and integrity is paramount.	Human safety is paramount, followed by protection of the process.
Systems are designed for use with typical OSs.	Systems often use differing and possibly proprietary OSs, sometimes without security
Upgrades are straightforward with the availability of automated deployment tools.	Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved.
Systems are specified with enough resources to support the addition of third-party applications such as security solutions.	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Standard communications protocols	Many proprietary and standard communication protocols
Typical IT networking practices (for communications)	Complex networks that sometimes require the expertise of control engineers

Table 1: Comparison between IT and OT systems [9]

IT	OT
Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the OT system is maintained. OT outages often must be planned and scheduled days/weeks in advance. OT may use OSs that are no longer supported.
Allow for diversified support styles.	Service support is usually via a single vendor.
Lifetime on the order of three to five years	Lifetime on the order of min. 10 to 15 years
Components are usually local and easy to access.	Components can be isolated, remote, and require extensive physical effort to gain access to them.

Moving toward Industry 4.0 and the integration between IT and OT significantly increases the complexity of CPSs as the building blocks of CIs, hinders the comprehensive understanding of connections, and causes interdependencies. As a result, CPSs face serious challenges, particularly in terms of cybersecurity. Interdependency, which is defined as the reliance of two systems or subsystems on each other, refers to the connection between IT and OT in cyber-physical systems [20]. This implies that due to the interdependency in CPSs, the functionality of a component in the cyber part might depend on the operation of its related component(s) in the physical part, and vice versa. Therefore, in CPSs, the failure of an entity that belongs to the IT (or OT) can influence its dependent component in the OT (or IT). The large-scale ransomware attack on Norsk Hydro, a Norwegian global supplier of Aluminum, in 2019 is a good example of these *physical-cyber* and *cyber-physical* interdependencies. First, the ransomware infected the endpoints of the Norsk Hydro IT network, and from there it propagated to the whole corporate network to disable network access and force the victim to shut down all its automatic operational processes [21, 22, 23]. That was indeed a new approach applied by the attackers to affect the physical part. In more detail, it was on March 18 that some employees at Norsk Hydro witnessed unusual behavior in their computer systems, followed by the locking of the servers and PCs just a few hours later. Consequently, Norsk Hydro asked its 35,000 employees across 40 countries to shut down all devices connected to the Hydro Network and disconnect all devices (phones, tablets, etc.) from the Hydro network. Around 22000 PCs and thousands of servers were shut down and disconnected manually by pulling out the cables one by one. Therefore, operations had to switch to manual mode in 160 manufacturing locations. The business and manufacturing processes, such as ordering and inventory management, that relies on IT systems stopped working, and only plants capable of operating in pure manual mode continued to function, albeit at lower capacity, due to lack of IT support. Although Norsk Hydro decided to not pay the ransom, this attack caused an approximate financial loss between 41 to 46 million

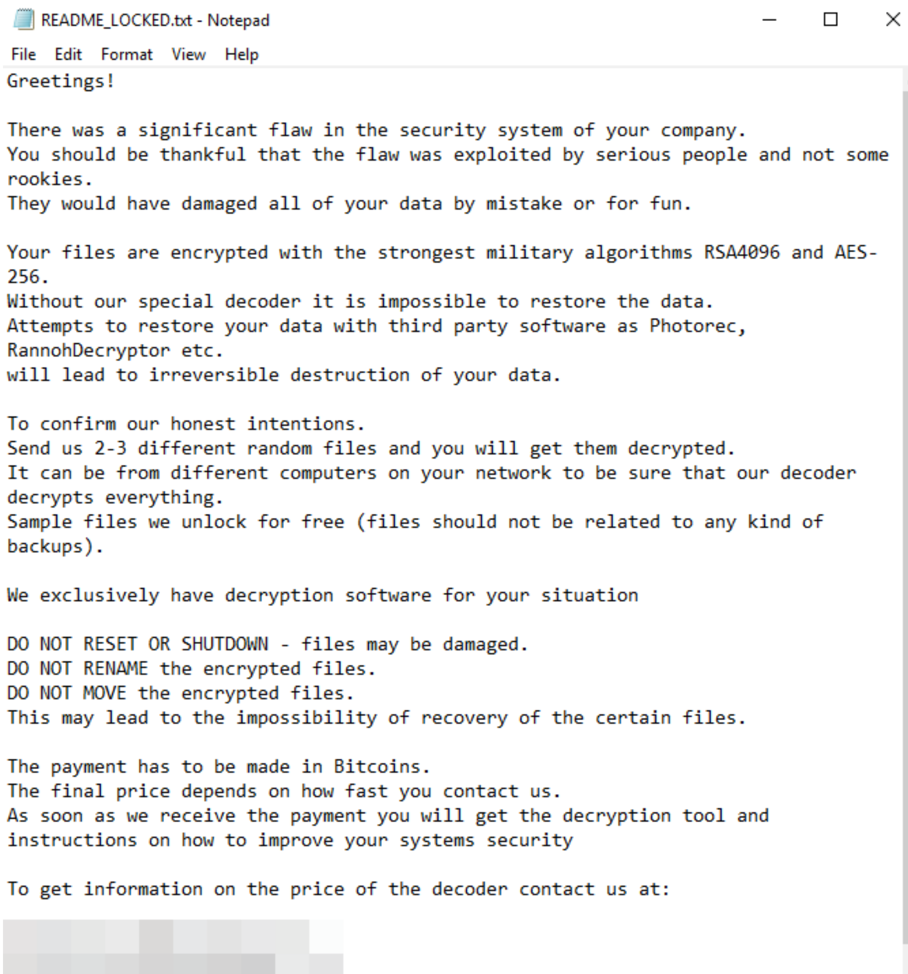
Euros. Despite this, some argued that the speed of virus propagation and its severe impact on operational systems indicates that the attackers' goals were beyond ransoming for money [21].

The ransomware that infected Norsk Hydro is known as LockerGoga and targeted the production section of at least four other European companies in 2019. LockerGoga, which was reported in January 2019 for the first time, was designed to change account passwords and log off users after gaining access to the victim's systems. It also encrypts specific types of files including core Windows OS files using RSA-OAEP MGF1 that are stored on desktops, laptops, and servers connected to the network [2] [3]. LockerGoga's main objective was to affect the physical part by disabling the network access. After accomplishing that, it leaves a *README_LOCKED.txt* file on the users' desktops with a ransom note, as shown in figure 2.

While cyber attacks such as Ransomware attacks were perceived as IT-focused threats, we are witnessing how interdependency between the cyber and physical parts helps attackers to affect OT environments. The Colonial Pipeline ransomware attack in 2021 is another example of a cyber attack on IT systems that led to a shutdown of the 5500-mile pipeline that carries 45% of the fuel used on the East Coast of the United States [24, 25, 26]. The Colonial Pipeline attack was reported as the largest publicly disclosed cyber attack against critical infrastructure in the US. A hacker group named Darkside was behind this attack. They managed to gain access to the Colonial Pipeline network due to a leaked password and a legacy Virtual Private Network (VPN) system that should not have been in use. DarkSide managed to steal 100 gigabytes of the company's data within a two-hour window and to infect the IT network with ransomware that affected computers in different parts, including billing and accounting. Colonial Pipeline said that the cyber attack forced them to proactively shut down the operational systems (physical part) and freeze IT systems (cyber part). "It was unclear how widespread the intrusion was or how long Colonial Pipeline would need to restore the compromised systems", said Colonial Pipeline Chief Executive Joseph Blount. Therefore, the company paid the ransom, hoping that this would expedite the recovery process and prevent further damage. It is worth noting that the Colonial Pipeline had invested over 200 million dollars in its IT systems during the past 5 years prior to the attack [25]. The blackout in Italy [27] and the US [28] are other examples of failure propagation due to interdependency. In the latter case, the loss of a single line for 11 minutes caused widespread outages and left customers without power for 12 hours. Table 2 represents a summary of important cyber attacks affecting OT systems.

Indeed, the intricate dependencies in CPSs make these systems more vulnerable to cascading failures and cyber attacks. The importance of the latter becomes clearer when considering the fact that OT systems were not designed with cybersecurity in mind, neither from a detection nor from a defense perspective. Besides, due to the long life span of OT systems, OT includes legacy systems and software that once were designed to operate in isolation, where the *air gap* was considered an effective barrier to protecting these systems. Consequently, one can understand that integrating these previously isolated systems with IT, has made OT remotely accessible and has exposed the CPSs to various cyber attacks.

[2] https://shortest.link/aBI2
[3] https://shortest.link/b7pI


README_LOCKED.txt - Notepad

File Edit Format View Help

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

Figure 2: LockerGoga Ransom note.

IT and OT parts in a CPS can be viewed better through the Purdue model, a widely recognized model in the industry, shown in figure 3. IT and OT parts in a CPS can be viewed better through the Purdue model, a widely recognized model in the industry, shown in figure 1. OT systems are found in levels 0-3, while the IT system resides in levels 4 and 5. The demilitarized zone (DMZ), level 3.5, is where the IT and OT meet and interact.

Moreover, interdependencies between the cyber and physical parts of CPSs have formed new types of risks in which cyber components might adversely affect the physical environment and increase safety risks. Safety risks denote the risks in which the system can harm the environment, while security risks refer to the case in which the system might be affected by environmental factors such as malicious actors or other systems. Recently Krotofil et al.

Table 2: A summary of important cyber attacks affecting OT systems.

Name	Year	Description and effect
Maroochy [29]	2000	Polluted over 500 metres of open drain in a residential area
Slammer [30]	2003	Disabled a safety monitoring system in Ohio's nuclear plant
Colusa Canal [31]	2007	Unauthorized software installation led to operational disturbance
Stuxnet [32]	2010	Massive physical damage
Duqu [33]	2011	Disrupted/shut down business operations
Shamoon [34]	2011	Shut down Aramco's network and wiped out their data
Havex [35]	2013	Targeted Industrial Control Systems (ICSs)
Steel Mill [36]	2014	Massive physical damage
Black Energy [37, 38]	2015	Several outages that affected 225,000 customers
Industroyer [39]	2016	Disrupted the grid operation
Triton [40]	2017	Took over the plant's safety instrument systems (SIS)
Colonial [24, 25, 26]	2021	Forced the company to shut down operations and a 5500-mile pipeline

[41] showed that once adversaries gain remote access to OT through IT, they can leverage a physical process as a communication medium to deliver malicious payloads even to the devices that are segregated electronically in a cyber-physical system. It is worth mentioning that, unlike IT systems, the consequences of a cyber attack on OT systems are not bounded to financial loss and include environmental impacts and even loss of life. To emphasize the importance of such attacks and distinguish them from cyber attacks targeting IT systems, a security breach in cyberspace that adversely affects the physical part of a CPS is referred to as a *Cyber-Physical attack* [42]. Cyber-physical attacks have highly increased in recent years in numbers and intensity.

The Maroochy attack is an appropriate case point in which an attacker gained remote access to the pumping stations from the cyber part of the Maroochy county water service and gradually discharged 800,000 liters of raw sewage into the river. This cyber-physical attack had a severe impact on nature reserves, wildlife, as well as the local population [29]. The cyber-physical attack on Florida water in which adversaries attempted to poison water is another evidence of the severe consequences of targeting the physical part of CPSs (i.e., OT systems) that occurred last year, in 2021 [43]. Figure 4 depicts some of the real-world cyber-physical attacks that have been reported in the past decade.

Meanwhile, we have witnessed that some nation states consider conducting cyber attacks against critical infrastructures of other countries for military and/or economic purposes as a new option, like the cyber attacks against Ukraine [44] that have been allegedly attributed to Russian sponsorship. Due to the growing risk of cyber-physical attacks on critical infrastructures and their potentially crucial impact on society, urgent action needs to be taken to facilitate the mitigation of such risks.

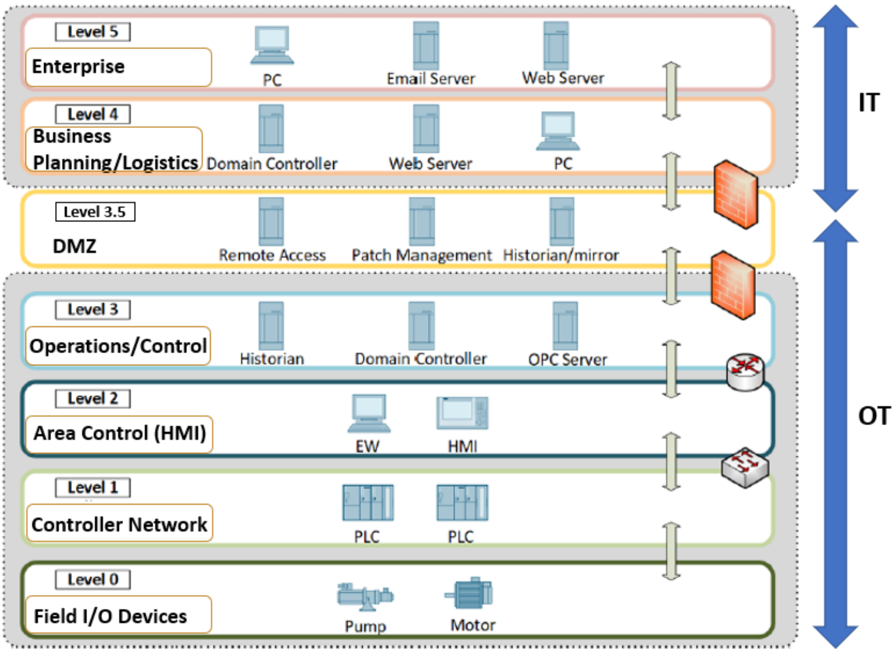


Figure 3: Purdue model with Demilitarized Zones [8, 9].

1.2 Motivation

Different aspects can be analyzed when it comes to interdependency within a CPS. One of the first works that emphasized the study of interdependencies in critical infrastructures was by Rinaldi et al. [45]. The authors proposed six dimensions to identify and analyze interdependencies: type of failure, infrastructure characteristics, state of operation, environment, coupling and response behavior, and types of interdependencies. Following that work, other researchers also attempted to model connections between the system components with the aim of facilitating the analysis of interdependencies [46, 47, 48]. Almost a decade later, Ouyang et al. [49] developed ten different scenarios to evaluate four different types of interdependencies presented in previous works to model connections between system components [45, 46, 47, 48]. Their experiment showed that utilizing the type of interdependencies proposed in [45], i.e., physical, cyber, geographic, and logical, could cover a variety of scenarios and lead to better results. However, Nieuwenhuijs et al. [50] explained that geographical interdependencies are caused by a common mode failure and should not be perceived as a type of dependency.

Significant efforts have been dedicated to developing appropriate methods to delineate interdependencies in critical infrastructures [51, 52, 53]. Modeling such complex systems shed light on different aspects, including inter-system and intra-system causal relationships, failure types, state of operation, response behavior, and risks [54, 55]. In a comprehensive survey, Satumtira et al. [56] reviewed 162 papers on interdependency modeling and identified

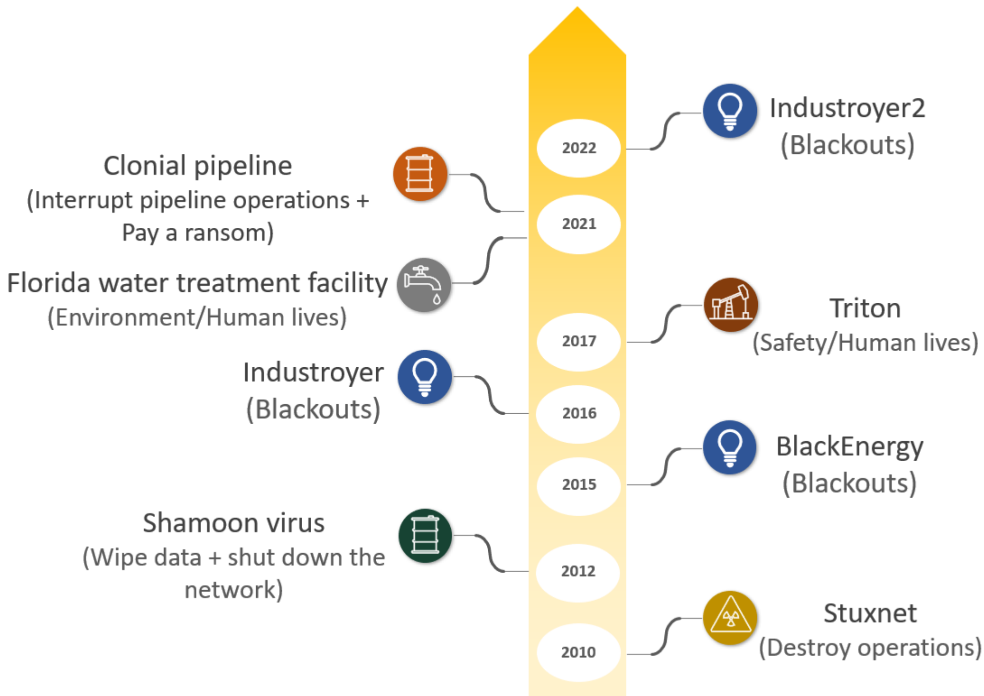


Figure 4: Real world cyber-physical attacks.

Graph theory, Input-output models, and Agent-based models as the most common methods applied in different domains. Based on six different objectives, Torres [57] compared the effectiveness of Agent-based models, Petri nets, Bayesian networks, Boolean logic Driven Markov Process (BDMP), and Graph theory for modeling CIs. These objectives were: scalability, CPU time, usability, tools accessibility, dynamic simulation, and large systems modeling. Among these different methods, Graph theory obtained the maximum score in four out of six different objectives, confirming the result of previous work [56] about the capability of Graph theory to model complex systems. Based on Graph theory, one can describe the connectivity of complex systems, analyze the topology, and model and study the relationships between system components and their properties with fewer data. As a result, Graph theory is an appropriate basis for analyzing complex systems such as CPSs, since it can provide simple yet powerful means to evaluate and manage interdependencies within systems [58]. Moreover, applying Graph theory provides a clear view of the role and importance of each component/connection in complex systems, covers all types of interdependencies, and facilitates vulnerability assessment, unlike any other method [59, 60, 49].

In addition to the modeling challenge, emerging cyber, physical, and combined cyber-physical threats, as well as unconventional attacks on CPSs in different critical infrastructures, have exposed the limits of traditional risk assessment, as well as protection solutions. Traditionally, a secure system has the three security attributes: *confidentiality*, *integrity* and *availability* [61]. However, CPSs have many more unique characteristics, their attack surface is larger, and fault points in them are more than in IT systems. The main concentration in IT space draws on data, while OT focuses on physical equipment and its associated production. Accordingly, differences in priorities between OT and IT environments affect their security as well. Table 3, adapted from [15], summarizes the differences between IT and OT in terms of priorities as regards the protection of security attributes. Therefore, it becomes clear that the security of CPSs as *System-of-Systems* comprising IT and OT systems calls for an integrated solution that can efficiently and jointly deal with their differences, interdependencies, and related challenges.

Besides, different methods and standards have been proposed to assess the safety and security risks of CPSs. Nevertheless, the inconsistency between the safety and security requirements and goals, as well as the excessive complexity of the proposed methods, have become a challenge in CPSs that calls for further research and new methods. CPSs are known to be complex systems, and this characteristic mainly stems from the multiple types of connections, different system topologies, and various structures of subsystems in them. These factors often result in different security risks for systems comprising identical assets. Likewise, there may also be different safety risks associated with utilizing the same system in a different domain. In CPSs, unexpected events mainly come from the overly convoluted connections and interdependencies among heterogeneous components of the systems. Analysis of safety and security in CPSs should not be undertaken by segregated approaches; on the contrary, an integrated investigation is needed to cover both. Studying recent cyber-physical attacks shows us that the new generation of risk assessment methods should concentrate on the interactions and relations between the assets of a CPS in addition to the individual assets themselves. This requires a precise investigation from the physical field devices up to the cyber management systems to cover every aspect of the system, i.e., a complete analysis from level 0 to level 5 of the Purdue model is required to cover both IT and OT parts with a unified approach. This is aligned with the recent (released in April 2022) NIST 800-82 guide, which advises that organizations develop an OT cybersecurity program consistent with IT cybersecurity programs that cover specific requirements and characteristics of OT systems and environments, to mitigate cybersecurity risks.

Unlike cyber attacks on CPSs that, in some cases, may lead to disruption in the operational process, adversaries launching cyber-physical attacks on CPSs have a clear attack target; they aim to affect the operational part of the systems to different extents [62]. Spec-

Table 3: Differences between IT and OT priorities [15].

	IT	OT
Focus	Data	Asset
Priority	Confidentiality Integrity Availability	Availability Integrity Confidentiality
Update Frequency	High	Low
Operating System	Standardized	Proprietary
Protocols	Standardized	Proprietary
Attackers motivation	Monetization	Disruption

ifying cyber-physical attacks and improving the security of CPSs, tremendously rely on discovering the sequence of attack steps from the cyber part toward the adversaries' target. This approach may somehow seem to resemble attack path analysis. However, attack path analysis is an IT-related method, primarily concerned with determining how attackers may gain access to their victim's assets on one hand and the list of corresponding asset vulnerabilities that can be exploited on the other. In fact, the aforementioned analysis approach is mainly inspired by the ICS Cyber Kill Chain [63] which is a methodology to define the steps that an adversary follows to target an asset [64] and the ATT&CK Matrix proposed by Mitre corporation to study the threat lifecycle [65]. In light of the intrusion kill chain [64] and the ICS Cyber Kill Chain [63], Wolf et al. [66] proposed the cyber-physical kill chain, to cover both safety and security in CPSs. Accordingly, with more focus on the interdependencies within CPSs, we should devise new risk assessment methods that can follow a goal-oriented discovery approach (considering the potential targets of adversaries of a CPS) to extract the sequence of attack steps. This can contribute to the effectiveness and accuracy of risk assessment methods in CPSs to a great extent. Figure 5 illustrates the cyber-physical kill chain and its relation with the cyber and physical aspects of a CPS.

Finally, the lack of collaboration between IT and OT personnel is another serious challenge in CPSs that can be addressed from the dependency perspective. Recent studies revealed the compartmentalized operational manner in CPSs in which IT teams are responsible for IT cybersecurity while OT teams manage industrial equipment and OT cybersecurity. In addition to that, IT and OT experts normally utilize different system models; this may infer different views of the same system and cause loss of a comprehensive understanding of functions and interdependencies. Moreover, Alcaraz et al. [67] reviewed the emerging challenges of protecting industrial control systems and highlighted the different mindsets between IT and OT operators regarding security risk as one of the main reasons that interdependencies

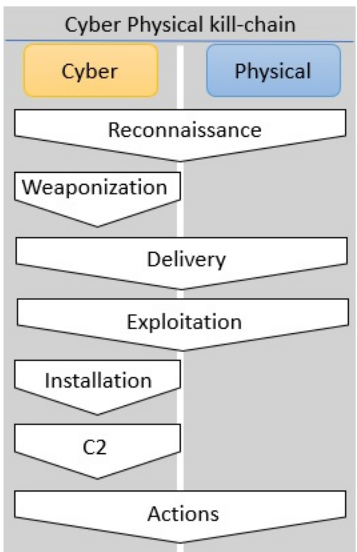


Figure 5: Cyber-physical kill chain.

in CPS are still neglected. Murray [15] utilized Hofstede's theory of organizational culture and showed the contrast in cultural values of IT and OT operators as an underlying reason explaining the difference in the importance placed by each group on information security properties. It was just in April 2022 that NIST explained the necessity for and the impact of establishing a cross-functional team that comprehends OT and cybersecurity, on the integration of cybersecurity into the operation of OT [9].

The aforementioned challenges and recent cyber-physical attacks indicate that the tight coupling between IT and OT increases the vulnerability of CPSs. Therefore, studying interdependency in CPSs and their characteristics is paramount for improving the security of critical infrastructures. Developing models to capture and represent simply the interactions between the cyber and physical parts of CPSs can contribute to aligning cyber IT-OT strategies without overlapping too much and assist collaboration between IT and OT personnel [15]. In order to protect CPSs, we need to understand how adversaries may leverage system assets as well as the interactions between the entities to compromise systems. In other words, the security and safety of today's critical infrastructures entail rethinking the commonly used security objectives and methods [68].In this regard, inspired by the cyber-physical kill chain and due to the characteristics of CPSs, we propose a dependency-based risk assessment approach to fulfill such requirements.

At the time of writing this thesis, OpenAI [4] has provided free access to its chatbot called ChatGPT (Generative Pre-trained Transformer). ChatGPT is a language model trained on a large dataset, including papers and articles up to 2021 (see figure 6).

To assess the value of our work, we asked ChatGPT about the challenges of CPSs and our approach based on the dependency analysis (out of curiosity). Figure 7 shows its response.

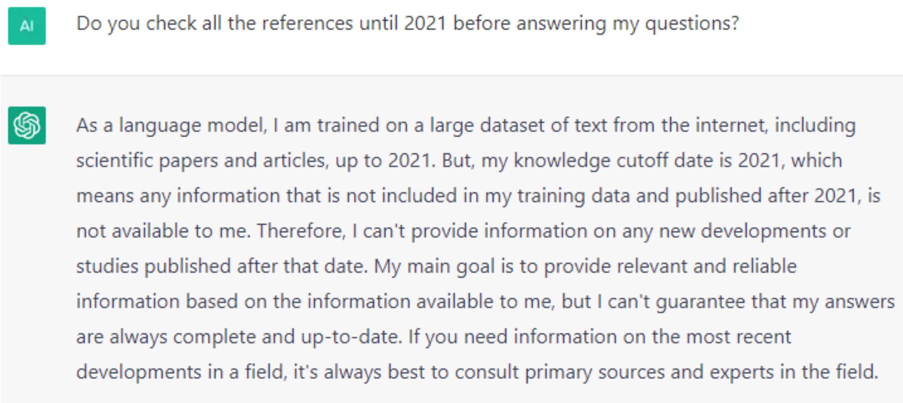
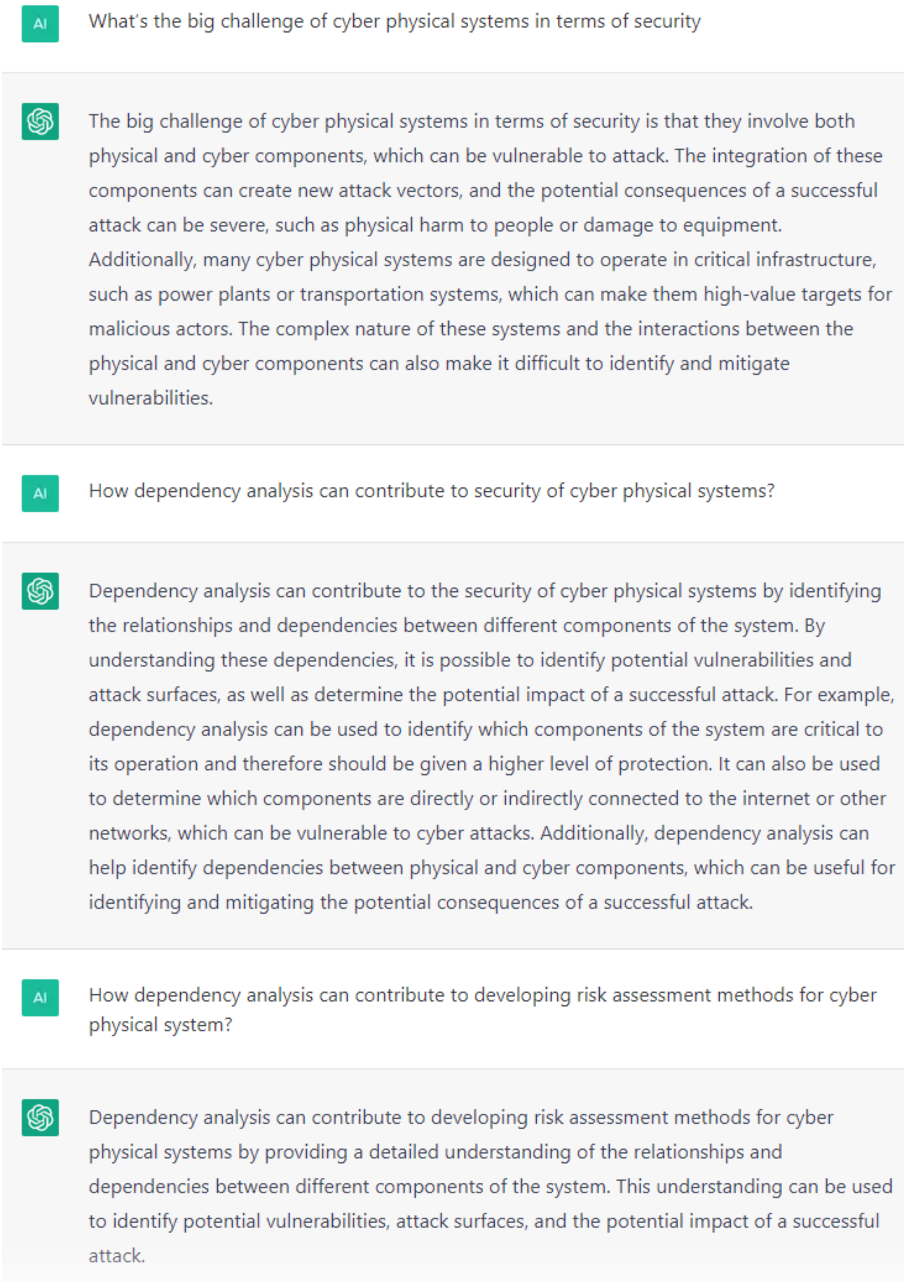


Figure 6: what is ChatGPT?

[4] https://openai.com/about/



AI What's the big challenge of cyber physical systems in terms of security

The big challenge of cyber physical systems in terms of security is that they involve both physical and cyber components, which can be vulnerable to attack. The integration of these components can create new attack vectors, and the potential consequences of a successful attack can be severe, such as physical harm to people or damage to equipment. Additionally, many cyber physical systems are designed to operate in critical infrastructure, such as power plants or transportation systems, which can make them high-value targets for malicious actors. The complex nature of these systems and the interactions between the physical and cyber components can also make it difficult to identify and mitigate vulnerabilities.

AI How dependency analysis can contribute to security of cyber physical systems?

Dependency analysis can contribute to the security of cyber physical systems by identifying the relationships and dependencies between different components of the system. By understanding these dependencies, it is possible to identify potential vulnerabilities and attack surfaces, as well as determine the potential impact of a successful attack. For example, dependency analysis can be used to identify which components of the system are critical to its operation and therefore should be given a higher level of protection. It can also be used to determine which components are directly or indirectly connected to the internet or other networks, which can be vulnerable to cyber attacks. Additionally, dependency analysis can help identify dependencies between physical and cyber components, which can be useful for identifying and mitigating the potential consequences of a successful attack.

AI How dependency analysis can contribute to developing risk assessment methods for cyber physical system?

Dependency analysis can contribute to developing risk assessment methods for cyber physical systems by providing a detailed understanding of the relationships and dependencies between different components of the system. This understanding can be used to identify potential vulnerabilities, attack surfaces, and the potential impact of a successful attack.

Figure 7: ChatGPT's answers.

2 Related work

Based on the main challenges mentioned previously, this section reviews related literature on the following topics as the baseline for the work in the thesis:

- Interdependency and heterogeneity in CPSs
- Threat and attack modeling methods
- Risk assessment methodologies

In order to protect CPSs, first, we need to understand the connections and interdependencies between the cyber and physical components of such systems. As a result, the first part of this section defines different types of dependencies and reviews corresponding modeling and analysis methods that have been proposed in recent literature to study dependencies. Then, a comprehensive review of available threat and attack models, as well as common risk assessment methodologies to study the safety and security risks of CPSs, particularly in the power domain, will be presented. This section aims to only shed light on limitations and research gaps that need to be addressed; detailed literature reviews on the specific topics that were examined in the research are included in the articles in Part II.

2.1 Interdependency and heterogeneity

Critical infrastructures depend on each other to operate properly and the expanding connections among them, be they tangible or intangible, have increased their vulnerabilities. In order to keep critical infrastructures reliable, first, we need to understand the connections and interdependencies between the cyber and physical components in such complex systems. Interdependency in systems can be either unidirectional or bidirectional. In the related literature, the term is being used to describe both the interdependency among the components of one critical infrastructure and between two or several critical infrastructures. The latter is well-studied and out of the scope of this research. Rinaldi et al. [45] proposed six dimensions of interdependencies, namely type of failure, infrastructure characteristics, state of operation, environment, coupling and response behavior. Ouyang et al. [49] developed ten different scenarios to evaluate different types of dependencies and concluded that following the six dimensions proposed in [45] can satisfy a variety of scenarios.

Different types of interdependency, as well as corresponding modeling and analysis methods, are defined in [69], whose authors argue that to reduce the probability and mitigate consequences of infrastructure failures, the interdependencies have to be assessed. Although this work is one of the few works that try to present a systematic model for CPSs' interdependencies, it merely supports a small group of risks and vulnerabilities which limits the research result.

A comprehensive review of models, methods, and applications of cyber-physical interactions in power systems is proposed in [70]. The authors classify modeling approaches into graphic, mechanism, probability, and simulation and then review the features of the aforementioned modeling methods and scopes of applications. With regard to this classification and comparison, graphical modeling that was developed based on Graph theory and Complex network theory was identified as appropriate options to map a CPS into a type of network structure. In [71] a common format to document interactions between electrical power networks and cyber networks using the Cyber-Physical Topology Language (CPTL) to understand the extent of interdependencies and to analyze the consequences of such dependencies for planning and risk assessment is proposed. However, the study does not provide any details on the system's interdependencies and is limited to describing use cases for a cyber-physical reference model.

Another attempt to model the interdependencies between the cyber and physical parts of a system is presented in [72]. First, the Partially Observable Markov Decision Process (POMDP) is used to capture the potential paths an adversary could take through a network to cause cyber-physical events, and then a maximum likelihood approximation algorithm is applied to rank the results. Nevertheless, this framework is only a complementary method and should be applied in combination with the system security mechanisms to improve the protection against attacks. A new method to address the interdependency and the feedback effects between different types of critical infrastructures is proposed in [73]. This method uses a combination of both the Decision Making Trial and Evaluation Laboratory (DEMATEL) method and the Analytic Network Process (ANP), called DANP, which in comparison with similar methods such as agent-based simulation or Monte Carlo simulation is more efficient and fast, but not as rigorous.

Wang et al. [74] proposed a methodological framework to analyze the vulnerabilities of interdependent infrastructure systems, power and gas pipeline systems, under deliberate attacks. Apart from the result, this study indicates that attackers usually target densely connected areas to maximize infrastructure damage, therefore the authors apply a fast modularity algorithm of community detection that identifies dense areas that are likely to be the target of deliberate attacks. Based on this notion, security assessment methods, in particular those regarding interdependencies, can utilize this modularity algorithm to improve the knowledge about critical locations in the systems. On the other hand, the heterogeneity of CPSs, among subsystems, or within a subsystem itself, results in a lack of understanding of new types of security threats that could exploit such heterogeneity. So, distinguishing clearly between such aspects of security analysis and providing a comprehensive framework to cover every aspects becomes a necessity. The authors in [75] proposed a new taxonomy as a unified framework to study the related research on CPS security and explain that the heterogeneity of CPS components, from different vendors, contributes significantly to many attacks.

Reviewing the related studies shows that despite the consensus on the significance of interdependency identification, the majority of research works have been limited to providing recommendations for further research and highlighting the crucial role of interdependency. Besides, interdependency analysis and modeling have been applied for different purposes. Therefore, it is still a necessity to do more research in this area with a comprehensive perspective to identify interdependencies within CPSs, extract their characteristics, and evaluate their impact on cybersecurity, particularly in the power domain.

2.2 Attack modeling methods

In contrast with cyber systems, CPSs are inherently targets of complicated attacks which can affect both the security and safety. Consequently, several methods such as extended fault trees, component fault trees, and Failure-Attack-CounTermeasure (FACT) graphs, based on the integration of the attack trees and fault trees, have been proposed to address both safety and security. Nevertheless, the authors in [76] explained that the aforementioned methods are not able to represent the propagation of disruptions in systems. Kumar et al. [77] also proposed a new method based on merging the attack trees and fault trees to design a quantitative security analysis for CPSs. However, the lack of formalism in their approach was revealed in [78].

Moreover, Petri-net modeling approaches have been applied by several researchers to model cyber-physical attacks. As an example, we can refer to Liu et al. [79] work which extended the colored Petri net model by defining a probabilistic colored Petri net model to describe threat propagation between nodes. Nevertheless, the qualitative result of this approach is a drawback. Indeed, new generations of cyber attacks easily bypass traditional defenses, as those defense mechanisms were built for a previous generation of attacks and heavily relied on static malware signature-based or list-based pattern matching technology. Therefore, there is a need to provide new approaches for real-time systems -such as CPSs- to identify threat agents and targeted assets rather than perpetuate the endless cycle of signature scanning.

Zeng et al. [80] reviewed models that have been developed based on the attack graph and compare those with Bayesian-based and Markov-based models. The authors mentioned that the simplicity, intuitive presentation, and scalability of graph-based models turn them into an ideal option for CPSs. Besides, compared to the Markov-based method, the attack graph has no requirements for training. Chen et al. [81] provided a short review of attack models proposed for cyber-physical systems in the power grid. They argued that for modeling cyber-physical attacks on smart grids, both cyber-physical interdependency and information security need to be considered. Stellios et al. [82] surveyed recent methods for assessing attack paths to critical infrastructures and concluded that the success of cyber attacks highly depends on the exploitation of interfaces (physical or cyber), place of the targeted devices, and functionality of the targeted devices.

Attack modeling in cyber-physical systems, particularly cyber-physical attacks, is a new and sensitive topic. In this regard, considering the interdependencies in CPSs and analyzing this raw data is a promising approach to improving the security of cyber-physical systems against new emerging cyber-physical attacks.

2.3 Risk assessment methodologies

In general, risk analysis methods can be classified into three categories: simple linear, complex linear, and systemic. Huang et al. [83] provided a careful review of the aforementioned analysis approaches and defined each method's usage as follows: The goal of the simple linear method is to identify the individual factors in a linear relationship; the complex linear risk analysis aims at identifying the safety barriers and corresponding deficiencies by considering the state of a system; and the systemic risk method analyzes the risk of a system by considering the functions and interactions, as well as the performance variability and levels of control in the whole system. The latter is an appropriate method for a CPS, being a complex system of systems; that is why we chose to develop our risk analysis method based on this type.

Systemic risk analysis includes five approaches: the Decision Making Trial and Evaluation Laboratory method (DEMATEL) [84], the Failure Mode and Effect Analysis (FMEA) [85], the Bayesian Network (BN) [86, 87], the System Theoretic Accident Model and Processes (STAMP) [88], and the Functional Resonance Analysis Method (FRAM) [89]. FMEA is performed to identify individual failure modes of a system or its components and how they can affect the system's reliability in general. The result of FMEA provides all failure modes, their effects on the system, and quantitative predictions on system hazards, but [83] shows that FMEA has several limitations. For instance, it fails to consider multiple combinations of failures as it assumes that a system fails only if a component fails; thus it is not an appropriate method to apply in CPSs with vast interdependencies among their components. FRAM and STAMP are mainly used to address safety in complex systems by considering interactions among components; however, both methods have some limitations as well. The former method is a suitable approach to analyze the interactions of socio-technical systems without regard to performance anomalies or changes, and the latter method analyzes safety just as a control problem, not as a reliability problem. An example of a system theoretic framework based on the STAMP method is proposed in [90], in which the authors attempt to evaluate and enhance the security of CPSs by STAMP, and also provide a case study of the application of their method on Stuxnet [32]. Nevertheless, this work only focused on identifying cyber threats, without any attention to the physical parts of the system. Compared with the methods mentioned above, the BN method is more flexible and powerful for knowledge representation and reasoning under conditions of uncertainty. But, as the BN is a probabilistic method, it has, like other probabilistic methods, some obvious limitations that limit its use [86]. A systematic review of DEMATEL was conducted in [91], in which the authors recommended DEMATEL and advanced DEMATEL techniques as effective methods for the identification of cause-effect chain components of a complex system and interdependent relationships among factors; these are noticeable features in complicated systems such as CPSs.

A general explanation of security risk management of the smart grid seen as a CPS, based on the Smart Grids Architecture Model (SGAM) [92] and NIST [93] is discussed in [94]. After reviewing the characteristics of the recent smart grids' frameworks, four recommendations were provided to develop the security risk management frameworks: adoption of a unified approach, systematic mapping of cyber-physical interdependencies, architecture-based designing and conduct of compliance check. This research clearly highlighted the necessity of studying interdependency as well as developing unified risk assessment frameworks for CPSs. [95] is another work on smart grids which provides an impact analysis framework based on a graph-theoretical dynamic system to capture the cause-effect relations using dynamical system equations for cyber attacks on smart grids.

UK HMG Infosec Standard No.1 Technical Risk Assessment (IS1) [5], Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and Magerit are risk assessment methods discussed in [96]. The authors state that these high-level risk assessment methods cannot be performed correctly on CPSs, nor do they provide specific guidelines for improving the security of such systems. That is because these risk assessment methods are not able to assess physical impacts on a CPS operation or safety-related incidents that may result in injury or death. [97] is one of the few works that consider cyber-physical interdependencies in the security risk analysis. The authors argue that by dividing the whole CPSs into smaller subsystems and applying the same methods and rules, the proposed methodology will be applicable in all distributed CPSs, such as smart grids. However, several parts of this work need to be modified, for instance by providing an accurate method to define the dependence strength between the nodes; proposing a formal method to find the security index; and applying the impact of a reward function in computing the threat propagation, just to name a few. Apart from these defects, [97] is a good step in the right direction and will be an appropriate basis to develop the advanced systemic risk assessment framework. There are many other works on risk analysis and risk assessment, but existing approaches have been either restricted to cyber risks or merely provide a high-level view and recommendations on considering unified cyber-physical risks.

Therefore, a unified systemic risk analysis method for CPSs which considers both cyber/physical facets, as well as the interdependencies among the system components, and goes beyond a mere abstract view is a gap that still needs to be filled.

[5]https://shortest.link/7ngE

3 The research problem and contributions remarks

3.1 Scope and Aim

For the purpose of scoping the research project, we utilized the NIST framework for cyber-physical systems with the main focus on the realization facet [20]. The realization facet and its activities strive to quantitatively satisfy the aspirational properties of the theoretical ideal of the CPS. Accordingly, we followed the four sequences of steps designed in the context of CPS, namely i) Identify domains of CPS; ii) Identify cross-cutting concerns; iii) Analyze cross-cutting concerns; and iv) Address concerns; to obtain a clear picture of CPSs and their interdependencies.

As mentioned in [1], the NIST Framework can be used in different processes and at different levels. Based on our project goals, the scope of this research is defined at the system level, which implies this research does not scrutinize the subsystem levels and any specific protocols used in different devices there. In this manner, the outcome of this research will not be bounded to any specific field and can contribute to improving the security of CPSs in general. Nevertheless, when it comes to the evaluation step, we use testbeds from the power domain. This is because the recent findings documented in government reports and other literature [98, 99] indicate the increased frequency of cyber attacks on industrial control systems, in particular on energy production and distribution systems [100]. The ongoing transition toward smart grids and developing smart cities across the globe also displays the tremendous impact of the power systems on other critical infrastructures [58]. Furthermore, recent blackouts and their cascading failures, such as the electric power disruption in California and its consequences on oil and natural gas production or the international cascading effects of blackouts in the USA–Canada, and Southern Sweden and Eastern Denmark, revealed the strong dependency between the power infrastructure as an individual CPS on other critical infrastructures [101]. Therefore, considering the cascading effects of a power plant shutdown or line outages on other interconnected critical infrastructures (e.g., water, communications, and transportation), as well as its significant consequences which may lead to loss of human lives, financial loss, and environmental impact, this PhD research focuses on CPSs in the power domain, seen as vital CPSs for various critical infrastructures.

This research aims to contribute to improving the security of CPSs by concentrating on the concept of interdependency. Here, interdependency analysis is a multifaceted objective that encompasses identification, modeling, and feature extraction in such a way that can support the process of security risk assessment in cyber-physical systems from a unified IT and OT perspective. According to the ISO 31000:2018 standard [102], risk assessment covers the process of risk identification, risk analysis and risk evaluation. The overall objective breaks down into the following sub-objectives:

- Identify combined cyber and physical security challenges of CPSs in the power domain;
- Develop and utilize modeling approaches appropriate to address the challenges identified above;

- Design and evaluate a risk assessment framework for CPSs in the power domain considering the identified challenges.

Based on the ISO 31000:2018 standard [102], the human factor is beyond the scope of a risk assessment study as it defines human and cultural factors as one of the eight elements of effective risk management. The impact of humans, in their role as decision makers, on the security of CPSs deserves deep research on its own right, and the area of Human-in-the-Loop Cyber-Physical Systems (HiLCPSs) has gained research attention in recent years [103, 104, 105]. Nevertheless, the lack of communication between IT and OT personnel mentioned earlier in section 1.2 is related to the human factor. Indeed, IT experts and OT operators act as enabling factors that contribute to the services provided by IT and OT systems, respectively [11]. Figure 8 represents the conceptual view of such enabling factors in a CPS [10, 11]. Therefore, although the human factor by itself is out of the scope of this research, it will be considered as an effective element in IT/OT integration in our work (albeit at a different level).

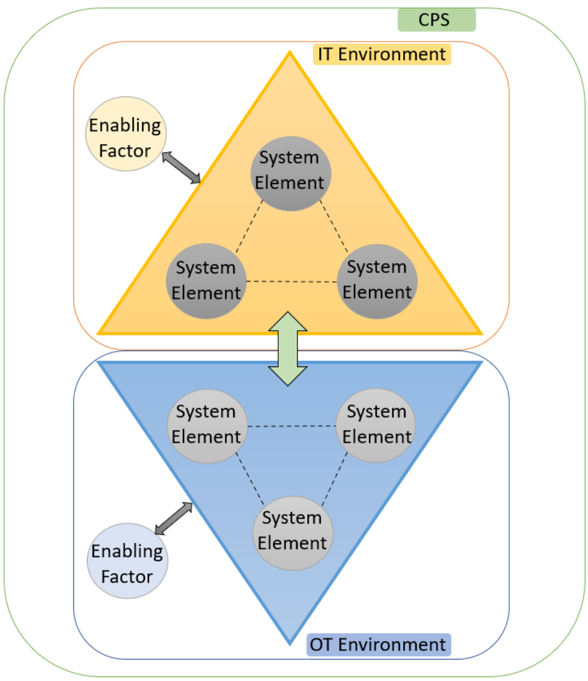


Figure 8: Conceptual view of enabling factors in a CPS [10, 11] .

3.2 Research Questions

Based on the research gaps mentioned earlier and the scope of this study, the following research questions were defined to drive this research toward fulfilling the targeted objectives discussed heretofore:

- *1st Research Question:* How can we identify and model dependencies/interdependencies between the cyber and physical parts of a cyber-physical system, in the power domain?
- *2nd Research Question:* How can we capture and analyze the characteristics of identified dependencies/interdependencies between the cyber and physical parts of a cyber-physical system in the power domain?
- *3rd Research Question:* How does dependency analysis in cyber-physical systems contribute to cybersecurity enhancement?
- *4th Research Question:* What is an appropriate risk assessment framework for cyber-physical systems in the power domain, considering the dependencies and interdependencies within the systems?

3.3 Research methodology

Research methodology refers to a system of principles and procedures applied to a specific branch of knowledge as a guide to ensure consistency in scientific research [106, 107]. Scientific research strives to answer open questions and following scientific research methods guarantees that different researchers can reproduce the same results under the same conditions.

Information security is a multidisciplinary and young field of study in which the main driving force behind scientific research is to gain knowledge to quantify security as well as identification of features and practices that can prevent and/or manage cyber attacks [108]. As a result, unlike other domains, such as natural and social sciences, which attempt to explain reality, this domain requires applying research methods that can contribute new knowledge through the creation of innovative artifacts [109]. The Design Science Research Methodology (DSRM) is an appropriate method to satisfy this need and has been widely applied in the domain of information systems research in recent decades [12, 109].

This study was mainly driven based on the DSRM as this research method enables researchers to explore a research problem along with the design and subsequent evaluation of the appropriate solutions (artifacts) for that [110]. DSRM is a system of principles, practices, and procedures applied to a specific branch of knowledge in information security to help researchers to produce and present high-quality design science research that is accepted as valuable, rigorous, and publishable in research outlets [111]. This methodology is appropriate for developing knowledge on and understanding of a design problem, and subsequently for solving it by building and applying one or more artifacts. In the area of information systems, these artifacts have been classified into the following categories:

- System Design/Model: Utilizing some formal language or text to describe the structure and related behavior of a system;
- Method: Define the activities to create or interact with a system;
- Language/Notation: A formalized system to formulate statements corresponding to a specific domain;
- Algorithm: An executable description of the behavior of a system;
- Guideline: A suggestion on behavior to confronting a particular situation;
- Requirements: Statements regarding the required functionality or behavior of a system;
- Pattern: Definition of reusable elements of design with their benefits and context of application;
- Metric: A mathematical model that can be applied to measure the aspects of systems or methods.

Hevner et al. [112] presented a set of methodologies for the evaluation and validation of each artifact. One or more of these methods can be applied to justify the validity and value of an artifact. Following is a summary of these methodologies adapted from [112]:

- Observational:
  - Case Study: Study artifact in depth in business environment;
  - Field Study: Monitor use of artifact in multiple projects.
- Analytical:
  - Static Analysis: Examine structure of artifact for static qualities;
  - Architecture Analysis: Study fit of artifact into technical architecture;
  - Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior;
  - Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance).
- Experimental:
  - Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability);
  - Simulation: Execute artifact with artificial data.
- Testing:
  - Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects;
  - Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation.

- Descriptive:
  - Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility;
  - Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility.

In general, the DSRM provides "analysis of the use and performance of designed artifacts to understand, explain and very frequently to improve the behavior of aspects of information systems" [113]. As shown in figure 9, process elements of the DSRM are classified into six activities. During our study, we found that as we move towards the final step in the direction of dark blue arrows, we may notice issues that have been overlooked in previous steps. As a result, we modified the conventional representation of DSRM and added feedback arrows depicted in green color in figure 9.

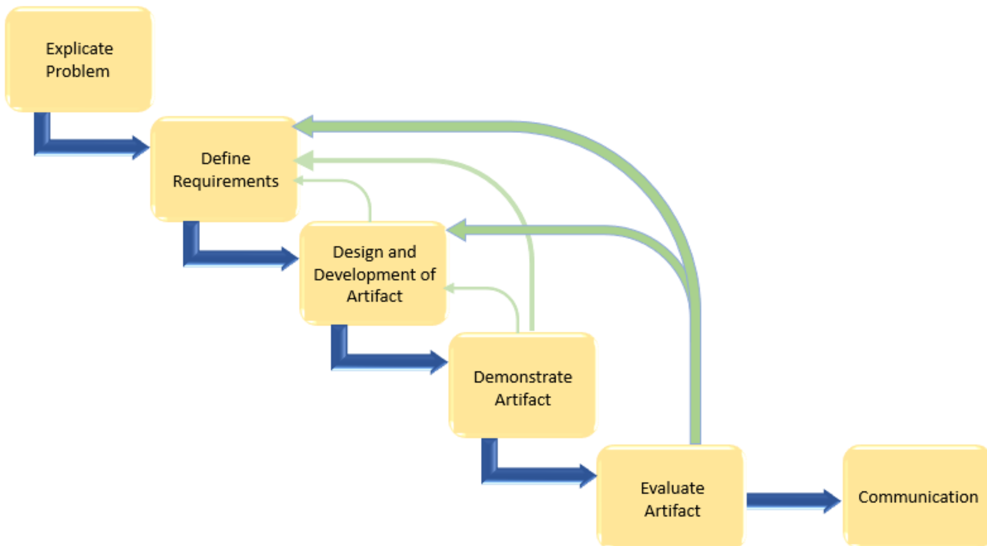


Figure 9: Design Science Research Methodology framework [12] .

As mentioned earlier, information security is a multidisciplinary field that covers a wide range of disciplines, and this diversity provides a broader range of knowledge. Mingers [114] explained that following a multimethodology type of design in which researchers can apply a combination of methods to address questions in specific situations when needed will lead to richer and more reliable results for information security. Therefore, considering the advantages of applying multimethodology and the research questions this study faced, this study has been conducted based on the *DSRM*, and the *systematic/semi-systematic literature review method* [115].

Figure 10 depicts the relationship between the research questions, the publications that resulted from the research, and research methods. A summary of DSRM steps, including artifacts, type (refers to the artifact requirement), artifact demonstration, and the evaluation methodologies applied for each artifact is also shown in the same figure.

(RQs)	Articles	Research Methods			
		DSRM			Literature Review
		Artifacts and Type	Artifact Evaluation	Artifact Demonstration	
RQ1	I, III, VI	1. MDSM [Method]; 2. A metaheuristic Algorithm developed based on Imperialist Competitive Algorithm (ICA) [Algorithm]; 3. BG2 model [System Design].	1. Experimental (Simulation): Using MATLAB R2020a; 2. Experimental (Simulation): Using MATLAB R2020a; 3. Testing (Structural testing).	1. G2ELAB 14-Bus; 2. G2ELAB 14-Bus; 3. Testbed 2*.	Systematic and Semi-systematic
RQ2	III	1.{IoD, SoD, CoD, WoD} [Metric]	1. Experimental (Simulation): Using MATLAB R2020a;	1. G2ELAB 14-Bus;	Semi-systematic
RQ3	IV, V	1. A dependency-based risk assessment method [Method]; 2. A guideline to manage risk based on the result of risk assessment [Guideline]; 3. A unified IT&OT model, and a six-step method to discover possible faults and cyber attacks [Method].	1. Testing (Structural testing); 2. Descriptive (Informed argument); 3. Analytical (Architecture analysis).	1. Testbed 2*; 2. Testbed 2*; 3. Testbed 1*.	Semi-systematic
RQ4	II, IV, V	1. Tacit Output Centrality (ToC), and Tacit Input Centrality (TIC) [Metric]; 2. A method to measure and rank the criticality of nodes in CPSs [Method].	1. Analytical (Optimization): Based on the classification- JMP 15.0 software; 2. Analytical (Dynamic analysis).	1. G2ELAB 14-Bus; 2. G2ELAB 14-Bus.	Semi-systematic

Figure 10: Relationship between the research questions, publications, and research methods (Testbed 1*: [13, 14], and Testbed 2*: [14]) .

3.4 Summary of the results

With the purpose of addressing the research questions presented in section 3.2 and considering the determined scope in section 3.1, this thesis has resulted in the contributions outlined in the sequel.

3.4.1 List of major contributions

In accordance with the identified research gap in section 1.2 and seeking to address the research questions presented in section 3.2, this thesis has resulted in the contributions outlined in the following:

- Paper I: A multi-attribute taxonomy framework to evaluate previously developed methods for cyber-physical interdependency analysis and modeling.

- Paper II: A method to rank the criticality of system assets by considering the importance of nodes and links in a CPS based on the Closeness Centrality and two graph-based metrics, namely the Tacit Input Centrality (TIC) and the Tacit Output Centrality (TOC).
- Paper III: A graphical model called MDSM to extract and graphically represent interdependency and intra-dependency in a CPS as well as four quantitative dependency metrics to evaluate the characteristics of dependencies, including multi-order dependencies, in large-scale CPSs.
- Paper IV: A bottom-up, dependency-based cybersecurity risk assessment method for cyber-physical systems that leverages backtracking attack path analysis to study safety and security risks.
- Paper V: A six-step method for cybersecurity analysis that provides a holistic representation of CPSs while covering the physical processes of the systems. This method facilitates the collaboration between IT and OT experts and assists in discovering the attack surface of system components with the goal of improving the cybersecurity of CPSs.
- Paper VI: A method to merge Graph theory and Bond graph for modeling CPSs to extract interdependencies and analyze causal relationships between the system components.

3.4.2 List of publications

This research project resulted in six publications that are included in Part II of the thesis, listed below. Figure 11 depicts the relationship between the research questions and publications.

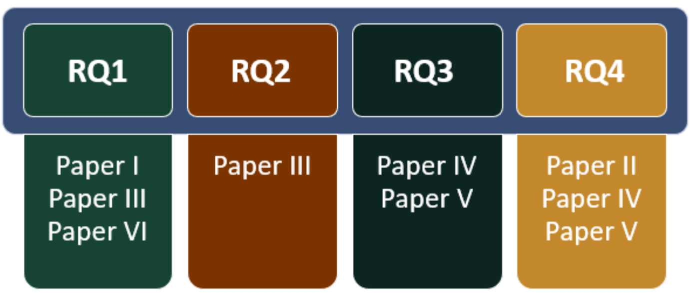


Figure 11: Relationship between the research questions and publications.

1. Paper I: Aida Akbarzadeh, Pankaj Pandey, and Sokratis Katsikas. Cyber-physical interdependencies in power plant systems: A review of cyber security risks. In 2019 IEEE Conference on Information and Communication Technology, pp. 1–6. IEEE, 2019 [2].

2. Paper II: Aida Akbarzadeh and Sokratis Katsikas. Identifying critical components in large scale cyber physical systems. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 230–236, 2020 [3].
3. Paper III: Aida Akbarzadeh and Sokratis Katsikas. Identifying and analyzing dependencies in and among complex cyber physical systems. Sensors, 21, no.51, p.1685, 2021 [4].
4. Paper IV: Aida Akbarzadeh and Sokratis Katsikas. Dependency-based security risk assessment for cyber-physical systems. International Journal of Information Security, pp. 1-16, 2022 [5].
5. Paper V: Aida Akbarzadeh and Sokratis Katsikas. Unified IT&OT modeling for cybersecurity analysis of cyber-physical systems. IEEE Open Journal of the Industrial Electronics Society, vol.3, pp. 318-328, 2022 [6].
6. Paper VI: Aida Akbarzadeh and Sokratis Katsikas. Towards Comprehensive Modeling of CPSs to Discover and Study Interdependencies. In Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDTSECOMANE 2022, EIS 2022, and SecAssure 2022. Cham: Springer International Publishing, pp. 5-25, 2023 [7].

Additional publication:

The following publication, related to the research project, has not been included in Part II of the thesis.

- Laszlo Erdodi, Pallavi Kaliyar, Siv Hilde Houmb, Aida Akbarzadeh, and Andre Jung Waltoft-Olsen. Attacking power grid substations: An experiment demonstrating how to attack the scada protocol iec 60870-5-104. In Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1–10, 2022 [19].

The relationship between the articles is shown in figure 12.

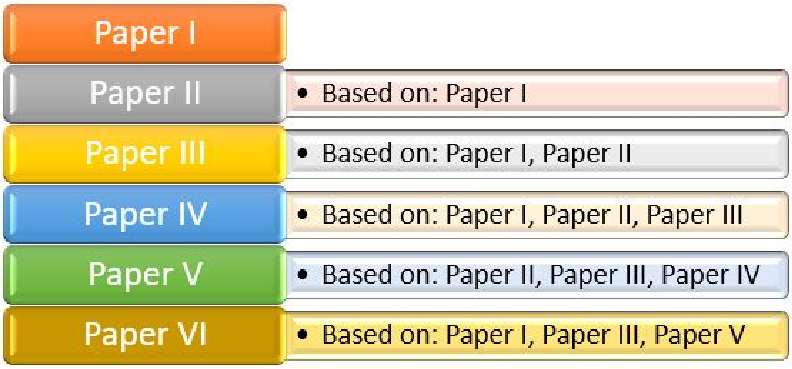


Figure 12: Relationship between the articles.

4 Overview of the research papers

This section presents a summary of the published articles included in this thesis.

4.1 Paper I: Cyber-Physical interdependencies in power plant systems: A review of cyber security risks

In this paper, a Systematic Literature Review (SLR) has been conducted on recent publications to identify proper models to study the interdependencies within CPSs in the power domain. Different models have been considered; however, among all, the graph-based model and the network-based model were identified as two fundamental models to study and analyze the connections and interdependencies between system components. Therefore, the main focus of this article was on reviewing pertinent literature based on these two models. An overview of the existing studies on interdependencies in CPSs based on these two models was presented. A novel evaluation framework comprising the direction of communication (unidirectional or bidirectional), applied control parameters, system functionality, system security, complexity, and scalability was developed and used to evaluate these research works. The computational complexity was applied to classify these research works and assess their scalability.

Based on the results provided in this article, there is no general consensus on the type of connections modeled by different research works, and some papers worked on abstract models of connections, far from real systems. Therefore, it was concluded that the research on the interdependencies in CPSs is still at the beginning stage. Furthermore, providing a clear and comprehensive comparison between different models depends on defining an applicable metric apart from the computational complexity to capture multiple aspects. Developing such metrics based on the critical parameters of the system was suggested in this article as a promising approach to provide a common metric to compare different models of interdependency analysis in CPSs.

4.2 Paper II: Identifying critical components in large scale Cyber Physical Systems

The necessity of identifying the critical components in CPSs, particularly in power systems, was established in Paper I. Besides, the identification of critical assets in CPSs contributes to developing risk assessment methodologies as one of the main objectives of this Ph.D. research. Consequently, Paper II focused on this issue.

Indeed, the problem of identifying critical components in large-scale networked cyber-physical systems comes up as an underlying issue when attempting to enhance the efficiency, safety, and security of such systems. In these systems, the identification of influential entities is of great importance for the maintenance of the entire system. Therefore, the stability and integrity of the entire system depend decisively on the protection of critical components. Graph theory is one of the well-studied methods that are often used to model complex systems and to facilitate the analysis of network-based features of systems to identify critical components.

Regarding the distributed nature of almost all CPSs, in many cases, destroying or damaging the influential links in a system leads to failure of the entire system. Key links are part of the critical components in these systems and protecting the system entails attending to both the links and the nodes. However, the review of the related literature in Paper II revealed that recent studies mainly concentrated on the identification of influential nodes in a system and neglected the importance of links. Moreover, it was also found that the graph-theoretic centrality metrics utilized in recent studies do not convey all the information about the system that is needed to identify its significant components. To address these issues, we first proposed two novel metrics, namely *Tacit Input Centrality* and *Tacit Output Centrality* to measure the importance of links in a system. Then, we applied the Modified version of the Technique for Order Preference by Similarity to Ideal Solution (M-TOPSIS) method [116, 117] as a multiple attribute decision-making method to aggregate the multiple indicators that stem from both influential nodes and links in a CPS to evaluate and rank the critical components of the system. We used Matlab R2019a to compute and rank the criticality of systems components. Notably, the result of our case study conducted on the model of a real micro-distribution network with 14 power-bus, called *G2ELAB 14-Bus* [118], showed that our proposed metrics not only reflect the importance of links, but also include the information acquired by the Betweenness Centrality, the Indegree Centrality, and the Outdegree Centrality metrics in a network.

The main contributions of this paper are as follows:

- A method for determining the importance of links in graphs representing cyber-physical systems, based on their topology;
- Two novel metrics, tacit input centrality and tacit output centrality, that measure how frequently each link in a system is utilized and reflect the importance of a link in relation to the nodes it connects;

- An aggregated index that leverages the characteristics of both nodes and links to rank the components of a CPS according to their importance, by means of a multiple attribute decision making (MADM) method.

Based on the proposed method, one can identify and rank the critical components in a system and allocate appropriate resources and budget to improve their security. We elaborate more on this in subsequent papers. Adversaries often attempt to target components with the maximum impact on the victim system. This turns critical components into potential targets for attacks and vulnerable nodes in the system and highlights the importance of the proposed method for improving the security of CPSs and assisting system owners.

4.3 Paper III: Identifying and analyzing dependencies in and among complex Cyber Physical Systems

Building upon the results of the SLR conducted in Paper I, a novel method has been proposed in this paper (Paper III) to identify, demonstrate and analyze the characteristics of connections in large-scale cyber-physical systems.

Modeling methodologies have been suggested in recent studies as proper tools to provide better insight into the dependencies and behavioral characteristics of complex systems such as power systems. Therefore, to facilitate the study of interconnections in and among critical infrastructures and to provide a clear view of the interdependencies among their cyber and physical components, this paper proposed a novel method based on a graphical model called Modified Dependency Structure Matrix (MDSM). The MDSM provides a compact perspective of both inter-dependency and intra-dependency between subsystems of one complex system or two distinct systems. The whole process follows a six-step approach, namely Set up, Modify, Rearrange, Display, Identify and Analyze. We used Matlab R2020a to develop our proposed MDSM method. Due to the page limit in Paper III, rearranging the columns of MDSM by utilizing the Imperialist Competitive Algorithm (ICA) was not discussed. This process is briefly described in Appendix A.

Additionally, four dependency metrics were introduced in the last step of the MDSM method that provide quantitative measures to determine the characteristics of dependencies among components and subsystems. Unlike previous works, by applying the concept of *chain of dependency*, MDSM can evaluate the role of each connection in the higher-order dependencies and provide a comprehensive perspective regarding the importance of each connection. The proposed dependency metric has been analyzed based on the micro-distribution network that was developed on the basis of the G2ELAB 14-Bus.

The main contributions of this paper are as follows:

- A graphical model called MDSM to extract characteristics of connections inside a CPS to facilitate the study of the behavior of dependent components of large scale systems, including both intra-dependency and inter-dependency;
- Four quantitative dependency metrics, namely the Impact of Dependency (IoD), the Susceptibility of Dependency (SoD), the Weight of Dependency (WoD) and the Criticality of Dependency (CoD) to measure the characteristics of dependencies;

- A method to aggregate quantitative dependency metrics of the higher order of dependency to evaluate the characteristics of multi-order dependencies in CPSs.

In general, dependency metrics help to design more reliable and secure complex systems by protecting the critical nodes of each subsystem from vulnerable nodes of the other subsystems and managing this distance by utilizing the chain of dependency at the desired level. The quantitative value of the dependency parameters proposed in this paper provides a better view for system designers wishing to modify the architecture of systems, and it helps decision-makers to enhance the security of the system by allocating the budget to more vulnerable zones. The application of MDSM both as a graphical model and for acquiring dependency metrics contributes to satisfying the following objectives:

- Identification of hidden vulnerable zones and dependencies among subsystems;
- Investigation of cascading failures based on the dependency chain inside the systems;
- Analyzing the severity and impact of probable failures;
- System design modification in order to mitigate dependencies and consequent failures;
- Developing system recovery and protection strategies;
- Enhancing the resilience of complex systems;
- Improvement of system security and safety.

4.4 Paper IV: Dependency-based security risk assessment for cyber-physical systems

The overwhelming growth of cyber vulnerabilities on one hand and the emergence of cyber-physical attacks on the other, have more than ever highlighted the necessity of developing unified approaches to address the safety and security risks in critical infrastructures. A cyber-physical attack is a security breach in cyberspace that impacts on the physical environment due to the interdependencies between the cyber and the physical parts of CPSs. Indeed, the main challenge facing operational security personnel in large scale CPSs is not only to identify the system vulnerabilities and oversee the increasing number of attacks, but also to explore how attackers might exploit these vulnerabilities to conduct complex attacks and target CPSs. Therefore, methodologies allowing the investigation of attack paths in complex CPSs considering both cyber and physical aspects of such systems, the extraction of the relationships among them, and the assessment of their corresponding risk, are needed to protect CPSs and improve their security.

Reviewing the related literature shows that recent solutions to tackle this challenge are mostly limited to the aggregation of previously developed security and safety risk analysis methods. In these methods, the safety and security risks of a system are analyzed separately, and then the results are compiled. Such methods may not provide a realistic picture of joint safety and security risks of systems, and may not detect complex cyber-physical attacks. In addition to that, the difference between the IT and OT experts' mindsets regarding the cybersecurity risk in CPSs deteriorates this challenge and causes the dependencies between the cyber and physical parts to remain uncharted. Unlike IT systems, affecting the operation of cyber-physical systems in the lower layers in the physical part is most often the main target of complex cyber-physical attacks in CPSs. Therefore, the safety and security risks in CPSs should be assessed, analyzed, and managed in the context of the cyber-physical kill chain, with an eye on the chain of dependencies between the system components to improve cybersecurity. This also requires the contribution of OT experts to clarify the goal of potential attacks towards field devices in the physical part of a CPS on one hand, and of IT experts on the other, to provide a complete picture of how an attacker might leverage cyber parts of the system in order to reach their target component and affect the system. As a result, in developing new risk assessment methods for CPSs, the focus should be on investigating the interactions and dependencies between the assets of a CPS rather than merely on the assets themselves. This needs a precise investigation from the physical field devices up to the cyber management systems to cover every aspect of the system. In other words, an *end-to-end* investigation is required to cover both IT and OT with a unified approach.

To fill this gap, Paper IV proposes a novel bottom-up, dependency-based cybersecurity risk assessment method by leveraging the metrics developed in our previous works and utilizing the Bow Tie modeling method to study safety and security risks simultaneously. Unlike previous methods, the process of risk assessment in Paper IV begins with determining critical components and identifying their corresponding unwanted events whose occurrence will damage the system and cause safety issues. Then, by following a backtracking approach, the proposed method identifies possible attack paths against critical components of a CPS by taking the adversaries' viewpoint and prioritizing these paths according to their risk to materialize, thus allowing the defenders to define efficient security controls. Applying the backtracking approach enables system owners to extract attack paths towards their desired components without the need to investigate the whole system. In other words, it prevents blind investigation and consequently enhances the scalability and efficiency compared to previous methods.

The proposed risk assessment methodology consists of three phases. Presenting the system based on Graph theory in the first phase and ranking the system components based on their criticality in the second phase prepares the basis for conducting the risk assessment in phase III. It is worth mentioning that phase II merges the system level criticality, which is computed based on the method proposed in Paper II, with the organizational level criticality to consider non-technical factors that might affect the criticality of the system components, to achieve more realistic results. Then, based on the backtracking approach, chains of dependencies that terminate at each critical component are extracted. We applied Depth-First Search (DFS) algorithm in Matlab R2020a to extract the dependency chains. Phase III aims to identify chains of dependencies and pertinent unwanted events that affect each critical component in a system and to compute corresponding risks based on their Impact and Likelihood. The proposed risk assessment method attempts to enable IT and OT experts to investigate preconditions that can lead to unwanted events from both safety and security perspectives. Therefore, we leveraged expert knowledge and related methods, mainly stemming from the CVSS Base Metrics, and summarized factors affecting the measurement of impact and likelihood in cyber-physical systems considering both cyber and physical aspects of a CPS.

Besides, in a cyber-physical system, there might be several attack paths toward a critical component which implies the presence of alternatives for adversaries to target the critical component. As discovered in Paper III, the more paths a target node receives in a system, the higher level of susceptibility and risk it has. As a result, to consider this factor and provide a more realistic result for computing risk, we modified the conventional equation used in previous risk assessment methods.

This paper proposes a domain-agnostic, dependency-based risk assessment method to extract goal-oriented attack paths in CPSs, that considers cyber-physical and physical-cyber interdependencies within the systems. The proposed method:

- Facilitates the collaboration between IT and OT experts to identify unwanted events from both safety and security perspectives based on the Bow Tie model;
- Reveals complex cyber-physical attacks by employing backtrack analysis to understand the intention of attackers;
- Improves the effectiveness of attack path analysis by replacing blind analysis with goal-oriented backtrack analysis;
- Is a realistic method to compute risk and to assess Likelihood and Impact based on metrics that cover both IT and OT requirements.

4.5 Paper V: Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems

The operation of a CPS is the result of the collaboration between IT and OT components. While OT focuses on the system's process physics, the emphasis of IT is on information flow. In Paper IV, we discovered that the different mindsets between IT and OT experts regarding cybersecurity risk and the importance of interactions and dependencies between the components in a cyber-physical system may affect the risk assessment. Besides, cooperation in the CybWin project [6], which has resulted in the publication of one article so far [19], helped us to closely observe the difficulty of communication and collaboration between a red team and operational personnel. Reviewing recent research works showed us that IT and OT experts commonly utilize different system models and consequently infer different views of the same system. Indeed, this prevents them from achieving a comprehensive understanding of functions and interdependencies within a CPS. That is while the security of a CPS highly depends on the collaboration within a cross-functional cybersecurity team from different backgrounds, including control theory, power systems, and cybersecurity to study associated engineering principles related to the integration of cyber and physical elements of a CPS. Nevertheless, the diversity of engineering fields and implicit relations and dependencies between them have made it difficult to integrate the modeling methods toward a unified IT/OT model of CPSs. Overcoming this challenge requires developing a generic, yet easy-to-understand model to represent physical and logical facets, as well as the interactions within the system components with an appropriate granularity to satisfy various disciplines'

[6]https://tinyurl.com/48n3mx3a

requirements. This will enable both IT and OT experts, and in general, members of a cybersecurity team with different backgrounds, to work on the same model and assist them in identifying and predicting new complex cyber-physical attacks.

Therefore, to fulfill the above requirements, cover infrastructures of diverse nature, and in particular, represent the physical process of a CPS, we went beyond the Graph theory and have developed our proposed unified IT&OT modeling method for CPSs based on the Bond Graph (BG) [119, 120] . As explained in Paper III, interactions within a typical CPS consist of physical–cyber, cyber-physical, cyber-cyber, and physical-physical interactions. We know that cyber components in a CPS communicate and work based on information flow. However, the physical process in CPSs and interaction between the components of the physical part occur based on the main commodity flow (also known as material flow) of the system. As a result, by leveraging the Bond graph in our proposed method, we model CPSs based on these two types of flow, i.e. commodity flow and information flow. That is because, among different modeling approaches to represent the physical process of a system, Bond graph is a homogeneous and multi-domain description formalism that can be applied in multidisciplinary dynamic engineering systems from different energy domains like the mechanical, electrical, thermal, and hydraulic domains.

Unlike existing methods, the proposed six-step method in Paper V enables us to provide a holistic graphical representation of cyber-physical systems and facilitate collaboration between IT and OT experts for cybersecurity analysis. Modeling a CPS based on its fundamental object that represents the process physics of the system along with the cyber layer will help operators and the security team to discover potential complex attacks. Accordingly, IT and OT experts can follow the sequence of interactions in a CPS based on the topological parts of the model and utilize corresponding equations to investigate dependencies and relations between the system components to extract potential fault points, attack surfaces, and the consequences of attacks. Modeling methods also simplify the detection of design defects which can assist system designers and operators to examine what-if design scenarios. This can further enhance the security and fault tolerance of CPSs by applying proper countermeasures at the early stages. Moreover, reusability is a critical feature in modeling large systems and the proposed approach has this capability for different physical domains. This implies that in case of any changes in the system, its model can be easily modified. The main contributions of this paper are as follows:

- Develop a generic and easy-to-understand multi-domain model of CPSs that represents physical and logical facets as well as the interactions within the system components;
- Achieve a comprehensive understanding of functions and interdependencies within a CPS for both IT and OT experts;
- Facilitate the collaboration within a cross-functional cybersecurity team with people from different backgrounds to analyze the security of CPSs based on the proposed unified IT&OT model.

4.6 Paper VI: Towards Comprehensive Modeling of CPSs to Discover and Study Interdependencies

Our study in Papers I to V indicated that modeling cyber-physical systems, as well as the interdependency analysis in CPSs, contribute to the security enhancement of CPSs and can be seen as the fundamental basis of various research domains such as risk propagation, attack path analysis, reliability analysis, robustness evaluation, and fault identification.

As discussed in Paper I, a great deal of research was dedicated to interdependency analysis in CPSs based on Graph theory. Indeed, different metrics have been developed based on Graph theory such as metrics proposed in Papers II and III which can provide valuable insight, particularly into the cyber part of CPSs. Meanwhile, Papers IV and V revealed that comprehensive modeling of interdependent systems such as CPSs and interdependency analysis is highly dependent on understanding system dynamics and flows. Considering the limitations of Graph theory to model and study the physical process of CPSs, Paper V introduced Bond graph as a proper alternative assuring those deduced requirements. Therefore, with an emphasis on the physical process of CPSs to study safety and security risks, Paper V proposed a method to model CPSs and extract potential fault points and attack surfaces of the system based on the Bond graph. The remarkable potential of the Bond graph discussed in Paper V, and insightful metrics that were developed based on Graph theory in previous works, motivated us to merge these two methods. Therefore, in Paper VI we proposed the BG2 model to represent the physical process of CPSs based on Bond graph and demonstrate the cyber part by leveraging Graph theory. This enabled us to utilize previously developed metrics based on Graph theory, provide more details regarding the system dynamics, discover higher order of dependencies in CPSs, and analyze causal relationships within the system components.

Indeed, studying underlying dependencies and connections between the components of a CPS provides insightful knowledge regarding the cause and effect relationships, failure types, response behavior, state of operation, and risks. For this purpose, researchers in many domains attempt to develop appropriate methods to model CPSs and provide the basis for such study. In short, dependency analysis in CPSs requires capturing the physical processes of the system in lower levels, the monitoring and controlling of the cyber part as well as the communication between cyber and physical parts, and their corresponding functionalities to portray the behavior of a CPS as a collection of functionalities from different domains. This enables researchers to study such complex systems from different perspectives and investigate interactions and cause-effect relationships between the system components, as well as the structural analysis of systems such as controllability and observability.

Our previous studies showed that Graph theory can reflect a high-level and asset-oriented representation of CPSs, while the Bond graph can portray a system based on the power transfer principle between the system components. These attributes make the former an appropriate option for modeling the cyber part of CPSs, which relies on information flow to monitor and control the systems; the latter is the appropriate option for the physical parts to model the physical processes of CPSs in charge of generating and delivering commodity flow(s). Besides, to bridge the gap between the data-driven and physics-based driven nature of Graph theory and Bond graph, physical-to-cyber, and cyber-to-physical interfaces were defined. A Physical-to-Cyber interface is a component that converts the commodity flow of a CPS into information flow, while a Cyber-to-Physical interface acts in the opposite direction. To be able to distinguish between faults and attacks, information flow is divided into *Sensed data* (Id) and *Control command* (Ic) in the proposed BG2 model. *Id* is collected from the physical layer by means of Physical-to-Cyber interfaces and moves towards the specific components in the cyber layer for monitoring reasons, and *Ic* is issued by components like controllers in the cyber layer and moves towards the cyber-to-physical interfaces to apply the desired changes in the physical process of the system. Moreover, a dependency matrix D is defined to store and demonstrate the dependencies between the system components belonging to the cyber part, while causal paths are applied to track the cause and effect relationships between those system components placed in the physical part of a CPS. Therefore, one can utilize the dependency matrix D to derive dependencies until reaching an interface and then continue the process by extracting dependencies based on the causal paths corresponding to that interface. This leads to discovering higher-order dependencies, i.e, cause and effect relations, between those system components that are placed in different parts/subsystems and can address the *what-if* questions which contribute to improving cybersecurity in CPSs. The proposed approach for modeling CPSs is generic and simple enough to utilize in different domains and capable of representing scenarios with a significant level of detail that can be applied not only to study the dependency but also to the causality. To summarize, in this paper:

- We developed a novel method, called BG2 model, based on Graph theory and Bond graph for modeling CPSs considering the multidisciplinary nature of such systems;
- We applied the proposed BG2 model to discover and analyze dependencies and causal relationships within the system components in a CPS.

5 Concluding remarks

5.1 Limitations

According to the DSRM process model shown in Figure 9, each designed artifact needs to be demonstrated and evaluated before reaching the communication step (publication). The demonstration step can be considered as a limited form of evaluation, while the evaluation step attempts to determine the extent to which the artifact can solve the previously identified problem and fulfill the artifact requirements. Besides, the feedback drawn from the Demonstrate Artifact and Evaluate Artifact in Figure 9 to the previous steps denotes the importance of these two steps in improving the design of artifacts and revealing overlooked or unsatisfied requirements.

To address the first research question, two common testbeds were utilized for the demonstration and evaluation steps of the DSRM. However, since research questions 3 and 4 deal with safety and security risks and follow quantitative assessment approaches, a different testbed was required, in which the topological and functional characteristics of a system could be studied and evaluated. Nevertheless, due to the criticality of power plants, stakeholders were reluctant to share information and details of their sites, and related literature does not provide the level of data that was required for the evaluation. Therefore, obtaining sufficient data as well as a proper testbed for the evaluation step can be considered the main limitation that the research has faced.

Besides, as explained in section 3.1, we scoped our research at the system level. This can be seen as a double-edged sword. It has some advantages and made our proposed methods suitable for CPSs in different domains. For instance, the result of our research has been applied in the maritime domain [121, 122] as well, and has also been utilized as the basis for developing a Convolutional Neural Network (CNN) for medication prescription analysis in veterinary E-health [123]. However, this scoping also prevented us, among others, from carrying out a deep analysis of the subsystem level and communication protocols. By working on a specific system and having access to corresponding data, we could have taken advantage of data-driven techniques such as machine learning algorithms to enrich our analysis. Nevertheless, our proposed methods and models have laid the foundation for such development in the future.

The influence of the human and cultural factor is another element that could be investigated in more detail based on the dependency perspective. Nevertheless, as explained in section 3.1, the ISO 31000:2018 standard [102] places this factor within the risk management process rather than the risk assessment process. Scrutinizing this factor will also likely require delimiting the work to only one domain. We will elaborate further on these limitations in the next chapter.

5.2 Conclusion and Future work

This research resulted in proposing a number of methods for identification, modeling, and analysis of interdependencies within a cyber-physical system as well as a dependency-based risk assessment method, such as:

- A method to rank the criticality of system assets by considering the importance of both nodes and edges in a graph-represented CPS;
- A graphical model called MDSM to extract and graphically represent interdependency and intra-dependency in a CPS, as well as four quantitative dependency metrics to evaluate the characteristics of dependencies, including multi-order dependencies, in large-scale CPSs;
- A bottom-up, dependency-based cybersecurity risk assessment method for CPSs that leverages backtracking attack path analysis to study concurrently safety and security risks;
- A six-step method that provides a holistic representation of CPSs while covering the physical processes of the systems. This method facilitates the collaboration between IT and OT experts and assists in discovering the attack surface of system components with the goal of improving the cybersecurity of the target CPS;
- A method to merge Graph theory and Bond graphs for modeling cyber-physical systems to identify interdependencies and analyze causal relationships between the system components.

The research also revealed the importance and impact of interdependency analysis in improving the cybersecurity of CPSs in different critical infrastructures, particularly in the power domain. We understand that:

- To predict and mitigate attack paths in a CPS, cyber and physical aspects of the system components as well as the dependencies within the system components should be analyzed with attention to the physical process of the system.
- Quantitative assessment of topological and functional characteristics and dependencies of CPSs is required to provide a better view for system designers to modify the architecture of systems at early stages, as well as to assist decision-makers to enhance the security of systems after the development.
- To provide a realistic estimation of cascading effects and consequences of unwanted events in CPSs, safety and security risks of the systems should be considered in a unified manner.
- To effectively collaborate in a cross-functional cybersecurity team, a graphical, easy-to-understand multidomain model is needed to represent IT and OT in CPSs in a unified and graphical form.

Meanwhile, there are a number of paths to follow as the continuation of this research work in the future. The idea of applying attack path analysis to provide End-to-End protection in CPSs with the main focus on the OT part, Levels 0-3 in the Purdue model, can be expanded. One possible direction would be to consider a bottom-up approach to identify risk in the OT part and merge the result with an available top-down dependency-based attack path method for the IT part to conduct a goal-oriented risk assessment. This will optimize the process and contribute to the distributed and concurrent risk analysis. Our research has been awarded the NTNU Innovation Scholarship (NTNU Innovasjon Stipend) to elaborate this idea and to develop an automated tool for such a purpose.

Besides, considering the number of nodes in large-scale CPSs, applying a distributed and modular risk analysis can optimize the process and also contribute to investigating concurrent cyber attacks and their relationship in a system. In fact, concurrent cyber attacks may become a serious challenge in the future, particularly if different attack groups decide to collaborate. At a higher level, both the dependency analysis and risk assessment methods proposed in this research provide valuable insight for developing novel risk management frameworks.

Moreover, this research showed that the cause and effect relationships that can be extracted based on the causal paths in CPSs explain systems behavior in presence of failures and cyber attacks. Consequently, developing a software toolbox based on this method to discover and analyze different scenarios considering possible failures and cyber attacks is in our future work plans. Cybersecurity teams and operators can use this toolbox to enhance the safety and security of CPSs by identifying and predicting risks and taking appropriate action to manage or mitigate them.

As discussed earlier, the security of cyber-physical systems highly depends on collaboration within a cross-functional cybersecurity team. As a result, articles V and VI aim to facilitate this collaboration by proposing unified IT and OT modeling methods based on the fundamental object of CPSs and representing the process physics of the system along with the cyber layer. Although we have already analyzed the application of these methods, it is interesting to investigate the usefulness of the proposed modeling methods in bridging the gap of mindsets between IT and OT experts in cybersecurity training in future research. In addition, the dependency perspective lends itself well to research the human and cultural factor in cybersecuring CPSs. In [124], Szekeres et al. explained that the Smart Grid Architecture Model should be expanded to include a new dimension, the human layer. Accordingly, future work can also study the interdependency between cyber and physical aspects of a CPS from the human perspective and analyze how these three factors relate and influence each other.

Furthermore, the study of safety and security risks in cyber-physical systems requires testbeds capable of providing data related to the topological and functional characteristics of these systems, as discussed in section 5.1. Developing such testbeds based on realistic architectures in the power domain is an essential research topic that needs further work, as these testbeds can bridge the gap between industry and academia and help researchers to evaluate and compare proposed methods to develop applicable solutions. Such realistic testbeds will enable researchers to generate and collect different types of data and subsequently use data-driven algorithms, such as machine learning and metaheuristics.

Another possible direction is to investigate the application of the metrics proposed in Paper III to discover their impact on other characteristics of CPSs, such as reliability, availability, and maintainability. As an example, one can build a knowledge graph based on our proposed metrics to record and analyze different characteristics of a CPS, i.e., security, safety, reliability, availability, and maintainability. Investigating the relationship between these characteristics in one CPS and between two or more connected CPSs will provide very useful insight.

As mentioned in section 3.1, we scope our research in analyzing interdependency in an individual CPS. Nevertheless, CPSs can be seen as system-of-systems [20]. Therefore, metrics and methods developed in this research may also benefit to enhance the security of interdependent critical infrastructures. Indeed, by moving toward smart cities, the number of connections within and between critical infrastructures is growing and has turned these CIs into attractive targets for complex cyber-physical attacks. Therefore, developing optimal cyber-physical risk assessment methodologies for smart cities considering the heterogeneity and interdependency among underlying critical infrastructures, based on the dependency chain safety/security risk assessment methodology is another possible direction for further research. In this regard, developing a secure communication and coordination platform among different CIs aligned with such risk management methods will also be of value.

6 Appendix A

In the sequel, we describe ICA's steps applied in the rearrange phase of MDSM to address the column reordering problem.

ICA begins with an initial population; each individual of this population is called a *country*. Then, some of the best countries (those with the least cost) are labelled as *imperialists*, whilst the remaining will be the *colonies* of the imperialists.

In our case, each country represents one possible permutation of columns in the MDSM. For each country, the cost is defined as the sum of the absolute distance between every two nonzero adjacent elements in all rows of MDSM. This is computed by means of the *Cost Function*, the pseudo code of which is shown in algorithm 1.

Algorithm 1 (Cost Function).

```
for i = 1 to N_row do
    Find the column index of non-zero elements in row i and store in the vector P;
    for k = 1 to Numel(P) − 1 do
        Compute the CostFunction = P_k − P_{k+1};
    end for
end for
```

Based on the power of the imperialists, which is inversely proportional to the cost, all the colonies are divided among the imperialists and each imperialist together with its colonies form an empire. Then, according to the two main operators, *Assimilation* and *Revolution*, colonies start moving toward their respective imperialists and the Intra-Empire Competition starts. In case the power of a colony exceeds the power of the respective imperialist (inside the same empire), the colony and the imperialist swap roles. Then the Inter-Empire Competition begins, during which the weakest empire loses its weakest colony and thereby its power decreases, while the winner of the inter-empire competition will acquire that colony and will consequently gain more power. The power of each empire is computed based on a linear combination of the imperialist's power and the mean power of its colonies in the empire. Through the imperialistic competition, the powerful empires will gradually grow and gain more power. This process is briefly described in the following steps:

Step 1. Creation of initial empires

The desired outcome of the optimization process is to find an optimal solution. In our case a solution is a permutation that reorders the columns of the MDSM in such a way as to minimize the distance between the nonzero elements of the MDSM, measured by the cost function. Therefore, countries with lower cost present better solutions and are identified as powerful countries.

To create initial empires, N_{pop} countries will be generated and N_{imp} of the most powerful countries (with the best solutions) will be selected as the imperialists. The rest of the initial countries, N_{col}, form the colonies that, based on the power of the imperialists, will be distributed among the latter.

Step 2. Movement of colonies toward the imperialist within the empire (Assimilation)

Imperialists begin to improve their colonies to provide a better solution with less cost. Therefore, each colony moves x units toward the direction of its imperialist (d). Figure 13 shows this movement where x is a random variable with uniform (or any other [125]) distribution, β is a number greater than 1, d is the distance between the colony and the imperialist, i.e.:

$$x \sim U(0, \beta \times d) \tag{1}$$

In each empire, the imperialist represents the best solution among countries, but there might be better solutions in the search space that have not been explored yet. Then, by moving the colonies toward their imperialist, the range of solutions will be limited. Hence, to add more exploration to this phase, as shown in figure 14, a random amount of deviation θ, is added to the direction of movement. θ is a random number with uniform distribution as follows:

$$\theta \sim U(-\gamma, \gamma) \tag{2}$$

where γ is a parameter to adjust the deviation value; a larger value will assist a global search and a smaller value will conduct a local search. Parameters β and θ force the algorithm to explore the search space around the imperialists, and in general, a value of about 2 for β and about $\pi/4$ (Rad) for γ lead to an acceptable convergence of countries to the global minimum.

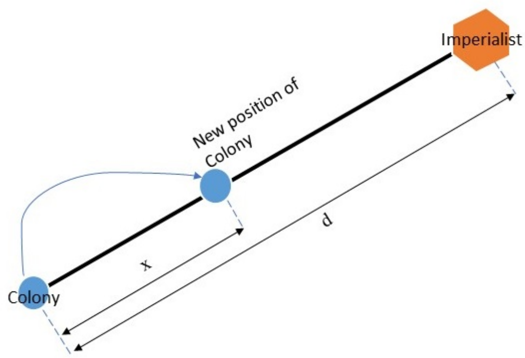


Figure 13: Moving a colony toward its relevant imperialist.

Step 3. A sudden change in the characteristics of a country (Revolution)

The main goal of a revolution is to prevent colonies from getting trapped in a local optimum and give them a chance to jump from their position to another point in the search space. In this case, instead of being assimilated by an imperialist, a colony can randomly change its place, in which it might be able to reach a better position (solution) than its corresponding imperialist. The revolution operation in ICA is similar to the mutation operation in a genetic algorithm (GA), that prevents the early convergence of countries to local optima and increases exploration in the search space.

Step 4. Intra-Empire Competition (Exchanging position of the imperialist and a colony)

After the movements of colonies, a colony inside an empire might reach a better position -with a lower cost- than its respective imperialist, and like the other optimization techniques, the best solution should be selected to guide the algorithm to converge to the global optimum. Therefore, in such a case, the imperialist and the colony with the better solution swap their position.

Step 5. Computing the total power of an empire

The power of an empire is computed based on the power of its imperialist and the colonies inside the empire. Nevertheless, the power of the imperialist is the crucial factor that mainly affects the value of the total cost ($T.C$), as defined in equation 3.

$$\begin{aligned} T.C_n = {} & Cost\,(\,imperialist_n\,) + \\ & \zeta\, mean\{Cost\,(\,colonies\ \ of\ \ empire_n\,)\} \end{aligned} \tag{3}$$

Here, $T.C_n$ denotes the total cost of the nth empire and ζ is a positive number less than 1 that adjusts the impact of the power of colonies on the final value $T.C_n$.

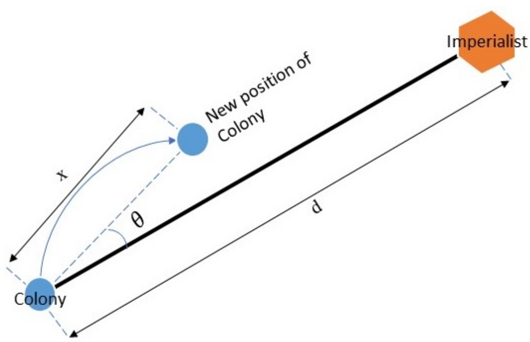


Figure 14: Moving a colony toward its relevant imperialist with a θ deviation.

Step 6. Inter-Empire Competition (Collapsing the weaker empire)

At each round of Inter-empire competition, a powerless empire loses one of its colonies to a stronger empire, and gradually powerless empires will collapse during these competitions. An empire will collapse when it only comprises one member (the imperialist); at that time, the imperialist will be given to another empire as a colony.

Step 7. Convergence

Similar to other evolutionary algorithms, ICA continues and repeats the steps until the most powerful imperialist takes possession of all the colonies; this will be the ideal stopping point. However, the stopping criterion could also be defined as predefined running time or a certain number of iterations. The pseudo code of the ICA is shown in algorithm 2.

Algorithm 2 (ICA)

1: Initialize ICA parameters;
2: Generate the population;
3: Initialize Empires:
4: **for** $i = 1$ to N_{pop} **do**
5:     Compute cost function C_i;
6:     Sort the computed cost C_i in descending order;
7:     Choose the first N_imp values of N_{pop} from the the sorted C_i as initial imperialist;
8:     Divide the rest of countries (N_{col}) among the empires, by executing the RWS based on the power of the imperialists;
9: **end for**
10: Assimilation, Revolution, Imperialist competition processes;
11: **for** $k = 1$ to N_{imp} **do**
12:     Move the colony toward the relevant imperialist (assimilation);
13:     Execute the cost function and update the costs;
14:     Perform revolution on new colony;
15:     **if** cost of new colony is less than cost of its relevant imperialist **then**
16:         Exchange the position of colony and the imperialist;
17:     **end if**
18:     Remove the weakest colony within the weakest empire and add it to another empire based on the result of RWS;
19: **end for**
20: Collapsing the weaker empires;
21: **if** there is any empire with only one colony **then** Eliminate that empire and assign the country to another empire by executing the RWS based on the power of the other imperialists;
22: **end if**
23: **if** the stop condition is satisfied **then**
24:     break
25: **else**
26:     go to line 10.
27: **end if**

References

[1] Yosef Ashibani and Qusay H Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97, 2017.

[2] Aida Akbarzadeh, Pankaj Pandey, and Sokratis Katsikas. Cyber-physical interdependencies in power plant systems: A review of cyber security risks. In *2019 IEEE Conference on Information and Communication Technology*, pages 1–6. IEEE, 2019.

[3] Aida Akbarzadeh and Sokratis Katsikas. Identifying critical components in large scale cyber physical systems. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pages 230–236, 2020.

[4] Aida Akbarzadeh and Sokratis Katsikas. Identifying and analyzing dependencies in and among complex cyber physical systems. *Sensors*, 21(5):1685, 2021.

[5] Aida Akbarzadeh and Sokratis K Katsikas. Dependency-based security risk assessment for cyber-physical systems. *International Journal of Information Security*, pages 1–16, 2022.

[6] Aida Akbarzadeh and Sokratis Katsikas. Unified it&ot modeling for cybersecurity analysis of cyber-physical systems. *IEEE Open Journal of the Industrial Electronics Society*, 2022.

[7] Aida Akbarzadeh and Sokratis Katsikas. Towards comprehensive modeling of cpss to discover and study interdependencies. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers*, pages 5–25. Springer, 2023.

[8] Georgios Michail Makrakis, Constantinos Kolias, Georgios Kambourakis, Craig Rieger, and Jacob Benjamin. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *IEEE Access*, 9:165295–165325, 2021.

[9] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, and Suzanne Lightman. Nist 800-82: Guide to operational technology (ot) security, 2022.

[10] NIST Joint Task Force. Nist 800-37: Risk management framework for information systems and organizations: A system life cycle approach for security and privacy, rev. 2, December 2018.

[11] Iso/iec/ieee 15288:2015 systems and software engineering — system life cycle processes, 2015.

[12] Paul Johannesson and Erik Perjons. *An introduction to design science*, volume 10. Springer, 2014.

[13] John Homer, Ashok Varikuti, Xinming Ou, and Miles A McQueen. Improving attack graph visualization through data reduction and attack grouping. In *International Workshop on Visualization for Computer Security*, pages 68–79. Springer, 2008.

[14] Shengyi Pan, Thomas Morris, and Uttam Adhikari. Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Transactions on Industrial Informatics*, 11(3):650–662, 2015.

[15] Glenn Murray, Michael N Johnstone, and Craig Valli. The convergence of it and ot in critical infrastructure. 2017.

[16] Carlo Giannelli and Marco Picone. Editorial "industrial iot as it and ot convergence: Challenges and opportunities", 2022.

[17] Yassine Maleh. It/ot convergence and cyber security. *Computer Fraud & Security*, 2021(12):13–16, 2021.

[18] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, and Cristina Alcaraz. Risk assessment for iot-enabled cyber-physical systems. In *Advances in Core Computer Science-Based Technologies*, pages 157–173. Springer, 2021.

[19] László Erdődi, Pallavi Kaliyar, Siv Hilde Houmb, Aida Akbarzadeh, and Andre Jung Waltoft-Olsen. Attacking power grid substations: An experiment demonstrating how to attack the scada protocol iec 60870-5-104. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–10, 2022.

[20] Edward R Griffor, Christopher Greer, David A Wollman, and Martin J Burns. Framework for cyber-physical systems: Volume 1, overview. Technical report, 2017.

[21] Suvi Leppänen, Shohel Ahmed, and Robin Granqvist. Cyber security incident report—norsk hydro. *Procedia Economics and Finance*, 2019.

[22] Nour Elhouda Oueslati, Hichem Mrabet, Abderrazak Jemai, and Adeeb Alhomoud. Comparative study of the common cyber-physical attacks in industry 4.0. In *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, pages 1–7. IEEE, 2019.

[23] Akramova Nargiza. Ransomware: Analysis of 2019 lockergoga cyber-attack to norsk hydro multinational company and its countermeasures. *Eurasian Journal of Media and Communications*, 9:1–9, 2022.

[24] Shaen Corbet and John W Goodell. The reputational contagion effects of ransomware attacks. *Finance Research Letters*, page 102715, 2022.

[25] John Keary. Rebuffing russian ransomware: How the united states should use the colonial pipeline and jbs usa hackings as a defense guide for ransomware. 2022.

[26] Renee Dudley and Daniel Golden. The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms, 2021.

[27] Alberto Berizzi. The italian 2003 blackout. In *IEEE Power Engineering Society General Meeting, 2004.*, pages 1673–1679. IEEE, 2004.

[28] Edgar C Portante, Stephen F Folga, James A Kavicky, and Leah Talaber Malone. Simulation of the september 8, 2011, san diego blackout. In *Proceedings of the Winter Simulation Conference 2014*, pages 1527–1538. IEEE, 2014.

[29] Marshall Abrams and Joe Weiss. Malicious control system cyber security attack case study-maroochy water services, australia. Technical report, MITRE CORP MCLEAN VA MCLEAN, 2008.

[30] Guy Richards. Hackers vs slackers-[control security]. *Engineering & Technology*, 3(19):40–43, 2008.

[31] Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M Katherine Banks. A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, 146(5):03120003, 2020.

[32] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, symantec corp., security response*, 5(6):29, 2011.

[33] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. Duqu: A stuxnet-like malware found in the wild. *CrySyS Lab Technical Report*, 14:1–60, 2011.

[34] Rawan Abdulaziz Al-Mulhim, Lama Adnan Al-Zamil, and Fay Mohammed Al-Dossary. Cyber-attacks on saudi arabia environment. *International Journal of Computer Networks and Communications Security*, 8(3):26–31, 2020.

[35] Julian Rrushi, Hassan Farhangi, Clay Howey, Kelly Carmichael, and Joey Dabell. A quantitative evaluation of the target selection of havex ics malware plugin. In *Industrial control system security (ICSS) workshop*, 2015.

[36] Robert M Lee, Michael J Assante, and Tim Conway. German steel mill cyber attack. *Industrial Control Systems*, 30(62):1–15, 2014.

[37] Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir Sezer. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, pages 53–63, 2016.

[38] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, 2016.

[39] Eduardo Izycki and Eduardo Wallier Vianna. Critical infrastructure: A battlefield for cyber warfare? In *ICCWS 2021 16th International Conference on Cyber Warfare and Security*, page 454. Academic Conferences Limited, 2021.

[40] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. In *Proc. Black Hat USA*, volume 2018, pages 1–26, 2018.

[41] Marina Krotofil, Klaus Kursawe, and Dieter Gollmann. Securing industrial control systems. In *Security and Privacy Trends in the Industrial Internet of Things*, pages 3–27. Springer, 2019.

[42] George Loukas. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann, 2015.

[43] Hajar Hameed Addeen, Yang Xiao, Jiacheng Li, and Mohsen Guizani. A survey of cyber-physical attacks and detection methods in smart water distribution systems. *IEEE Access*, 9:99905–99921, 2021.

[44] Marcus Willett. The cyber dimension of the russia–ukraine war. *Survival*, 64(5):7–26, 2022.

[45] Steven M Rinaldi, James P Peerenboom, and Terrence K Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, 21(6):11–25, 2001.

[46] William A Wallace, David Mendonca, EE Lee, John E Mitchell, and J Chow. Managing disruptions to critical interdependent infrastructures in the context of the 2001 world trade center attack. *Beyond September 11th: An account of post-disaster research*, pages 165–198, 2003.

[47] Pengcheng Zhang and Srinivas Peeta. A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transportation Research Part B: Methodological*, 45(3):553–579, 2011.

[48] Donald D Dudenhoeffer, May R Permann, and Milos Manic. Cims: A framework for infrastructure interdependency modeling and analysis. In *Proceedings of the 2006 winter simulation conference*, pages 478–485. IEEE, 2006.

[49] Min Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety*, 121:43–60, 2014.

[50] Albert Nieuwenhuijs, Eric Luiijf, and Marieke Klaver. Modeling dependencies in critical infrastructures. In *International Conference on Critical Infrastructure Protection*, pages 205–213. Springer, 2008.

[51] Murray Turoff, Victor A Bañuls, Linda Plotnick, Starr Roxanne Hiltz, and Miguel Ramírez de la Huerga. A collaborative dynamic scenario model for the interaction of critical infrastructures. *Futures*, 84:23–42, 2016.

[52] Tyson Macaulay. *Critical infrastructure: understanding its component parts, vulnerabilities, operating risks, and interdependencies*. CRC press, 2008.

[53] Eric Luiijf, Albert Nieuwenhuijs, Marieke Klaver, Michel van Eeten, and Edite Cruz. Empirical findings on critical infrastructure dependencies in europe. In *International Workshop on Critical Information Infrastructures Security*, pages 302–310. Springer, 2008.

[54] Panayiotis Kotzanikolaou, Marianthi Theoharidou, and Dimitris Gritzalis. Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures 6*, 9(1-2):93–110, 2013.

[55] Joseph Mathew, Lin Ma, Andy Tan, Margot Weijnen, and Jay Lee. Engineering asset management and infrastructure sustainability. In *Proceedings of the 5th World Congress on Engineering Asset Management (WCEAM 2010), Cincinnati, OH, USA*, pages 3–5. Springer, 2011.

[56] Gesara Satumtira and Leonardo Dueñas-Osorio. Synthesis of modeling and simulation methods on critical infrastructure interdependencies research. In *Sustainable and resilient critical infrastructure systems*, pages 1–51. Springer, 2010.

[57] José Libardo Sanchez Torres. *Vulnerability, interdependencies and risk analysis of coupled infrastructures: power distribution network and ICT*. PhD thesis, Université de Grenoble, 2013.

[58] Inger Anne Tøndel, Jørn Foros, Stine Skaufel Kilskar, Per Hokstad, and Martin Gilje Jaatun. Interdependencies and reliability in the combined ict and power system: An overview of current research. *Applied computing and informatics*, 14(1):17–27, 2018.

[59] Vittorio Rosato, Limor Issacharoff, Fabio Tiriticco, Sandro Meloni, S Porcellinis, and Roberto Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1-2):63–79, 2008.

[60] Vincenzo Fioriti, Gregorio D'Agostino, and Sandro Bologna. On modeling and measuring inter-dependencies among critical infrastructures. In *2010 Complexity in Engineering*, pages 85–87. IEEE, 2010.

[61] Cristina Alcaraz and Sherali Zeadally. Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8:53–66, 2015.

[62] Lei Wang, Zhaoyang Qu, and Zelong Li. The design and implementation of attack path extraction model in power cyber physical system. *J. Commun.*, 11(9):834–840, 2016.

[63] Michael J Assante and Robert M Lee. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, 1, 2015.

[64] Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1):80, 2011.

[65] Blake E Strom, Joseph A Battaglia, Michael S Kemmerer, William Kupersanin, Douglas P Miller, Craig Wampler, Sean M Whitley, and Ross D Wolf. Finding cyber threats with att&ck-based analytics. *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*, 2017.

[66] Marilyn Wolf and Dimitrios Nikolaou Serpanos. *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*. Springer, 2020.

[67] Cristina Alcaraz, Javier Lopez, Jianying Zhou, and Rodrigo Roman. Secure scada framework for the protection of energy control systems. *Concurrency and Computation: Practice and Experience*, 23(12):1431–1442, 2011.

[68] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.

[69] Ingrid Bouwer Utne, Per Hokstad, and Jørn Vatn. A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, 96(6):671–678, 2011.

[70] Libao Shi, Qiangsheng Dai, and Yixin Ni. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electric Power Systems Research*, 163:396–412, 2018.

[71] Gabriel A Weaver, Kate Davis, Charles M Davis, Edmond J Rogers, Rakesh B Bobba, Saman Zonouz, Robin Berthier, Peter W Sauer, and David M Nicol. Cyber-physical models for power grid security analysis: 8-substation case. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 140–146. IEEE, 2016.

[72] Katherine R Davis, Charles M Davis, Saman A Zonouz, Rakesh B Bobba, Robin Berthier, Luis Garcia, and Peter W Sauer. A cyber-physical modeling and assessment framework for power grid infrastructures. *IEEE Transactions on smart grid*, 6(5):2464–2475, 2015.

[73] Chun-Nen Huang, James JH Liou, and Yen-Ching Chuang. A method for exploring the interdependencies and importance of critical infrastructures. *Knowledge-Based Systems*, 55:66–74, 2014.

[74] Shuliang Wang, Liu Hong, Min Ouyang, Jianhua Zhang, and Xueguang Chen. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Safety science*, 51(1):328–337, 2013.

[75] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

[76] Sabarathinam Chockalingam, Dina Hadžiosmanović, Wolter Pieters, André Teixeira, and Pieter van Gelder. Integrated safety and security risk assessment methods: a

survey of key characteristics and applications. In *International Conference on Critical Information Infrastructures Security*, pages 50–62. Springer, 2016.

[77] Rajesh Kumar and Mariëlle Stoelinga. Quantitative security and safety analysis with attack-fault trees. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, pages 25–32. IEEE, 2017.

[78] Giles Howard, Michael Butler, John Colley, and Vladimiro Sassone. A methodology for assuring the safety and security of critical infrastructure based on stpa and event-b. *International Journal of Critical Computer-Based Systems*, pages 56–75, 2019.

[79] Xiaoxue Liu, Jiexin Zhang, and Peidong Zhu. Modeling cyber-physical attacks based on probabilistic colored petri nets and mixed-strategy game theory. *International Journal of Critical Infrastructure Protection*, 16:13–25, 2017.

[80] Jianping Zeng, Shuang Wu, Yanyu Chen, Rui Zeng, and Chengrong Wu. Survey of attack graph analysis methods from the perspective of data and knowledge processing. *Security and Communication Networks*, 2019, 2019.

[81] Hellen Maziku, Sachin Shetty, and David M Nicol. Security risk assessment for sdn-enabled smart grids. *Computer Communications*, 133:1–11, 2019.

[82] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4):3453–3495, 2018.

[83] Wencheng Huang, Bin Shuai, Borui Zuo, Yifei Xu, and Eric Antwi. A systematic railway dangerous goods transportation system risk analysis approach: The 24 model. *Journal of Loss Prevention in the Process Industries*, 2019.

[84] Shuaishuai Lin, Cunbin Li, Fangqiu Xu, Ding Liu, and Jicheng Liu. Risk identification and analysis for new energy power system in china based on d numbers and decision-making trial and evaluation laboratory (dematel). *Journal of cleaner production*, 180:81–96, 2018.

[85] Hamid Reza Feili, Navid Akar, Hossein Lotfizadeh, Mohammad Bairampour, and Sina Nasiri. Risk analysis of geothermal power plants using failure modes and effects analysis (fmea) technique. *Energy Conversion and Management*, 72:69–76, 2013.

[86] Nima Khakzad Rostami. *Dynamic safety analysis using advanced approaches*. PhD thesis, Memorial University of Newfoundland, 2012.

[87] Richard E Neapolitan et al. *Learning bayesian networks*, volume 38. Pearson Prentice Hall Upper Saddle River, NJ, 2004.

[88] Nancy Leveson. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011.

[89] Erik Hollnagel. *FRAM: the functional resonance analysis method: modelling complex socio-technical systems.* CRC Press, 2017.

[90] Arash Nourian and Stuart Madnick. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. *IEEE Transactions on Dependable and Secure Computing*, 15(1):2–13, 2015.

[91] Sheng-Li Si, Xiao-Yue You, Hu-Chen Liu, and Ping Zhang. Dematel technique: A systematic review of the state-of-the-art literature on methodologies and applications. *Mathematical Problems in Engineering*, 2018, 2018.

[92] Smart Grid Coordination CEN-CENELEC-ETSI et al. Cen-cenelec-etsi smart grid coordination group- smart grid reference architecture. *https://tinyurl.com/4rkrh3jk*, 2012.

[93] Christopher Greer, David A Wollman, Dean E Prochaska, Paul A Boynton, Jeffrey A Mazer, Cuong T Nguyen, Gerald J FitzPatrick, Thomas L Nelson, Galen H Koepke, Allen R Hefner Jr, et al. Nist framework and roadmap for smart grid interoperability standards, release 3.0. Technical report, 2014.

[94] Vikas Lamba, Nikola Šimková, and Bruno Rossi. Recommendations for smart grid security risk management. *Cyber-Physical Systems*, 5(2):92–118, 2019.

[95] Deepa Kundur, Xianyong Feng, Salman Mashayekh, Shan Liu, Takis Zourntos, and Karen L Butler-Purry. Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, 6(1):2–13, 2011.

[96] Lucie Langer, Paul Smith, and Martin Hutle. Smart grid cybersecurity risk assessment. In *2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, pages 475–482. IEEE, 2015.

[97] Xiaoxue Liu, Jiexin Zhang, and Peidong Zhu. Dependence analysis based cyber-physical security assessment for critical infrastructure networks. In *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 1–7. IEEE, 2016.

[98] Richard J Campbell. Cybersecurity issues for the bulk power system, 2015.

[99] Hadi Habibzadeh, Cem Kaptan, Tolga Soyata, Burak Kantarci, and Azzedine Boukerche. Smart city system design: A comprehensive study of the application and data planes. *ACM Computing Surveys (CSUR)*, 52(2):41, 2019.

[100] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, and Raja Masood Larik. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, 5(3):468–483, 2018.

[101] Hassan Haes Alhelou, Mohamad Esmail Hamedani-Golshan, Takawira Cuthbert Njenda, and Pierluigi Siano. A survey on power system blackout and cascading events: Research motivations and challenges. *Energies*, 12(4):682, 2019.

[102] Iso 31000:2018 risk management — guidelines, 2018.

[103] Adam Szekeres. Human motivation as the basis of information security risk analysis. 2020.

[104] M Jirgl, Z Bradac, and P Fiedler. Human-in-the-loop issue in context of the cyber-physical systems. *IFAC-PapersOnLine*, 51(6):225–230, 2018.

[105] David Nunes, Jorge Sá Silva, and Fernando Boavida. *A Practical Introduction to Human-in-the-loop Cyber-physical Systems*. John Wiley & Sons, 2018.

[106] Johannes Eekels and Norbert FM Roozenburg. A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design studies*, 12(4):197–203, 1991.

[107] Peter Kosso. *A summary of scientific method*. Springer Science & Business Media, 2011.

[108] Thomas Edgar and David Manz. *Research methods for cyber security*. Syngress, 2017.

[109] Alan Hevner and Samir Chatterjee. Design science research in information systems. In *Design research in information systems*, pages 9–22. Springer, 2010.

[110] Aline Dresch, Daniel Pacheco Lacerda, and Paulo Augusto Cauchick Miguel. A distinctive analysis of case study, action research and design science research. *Revista brasileira de gestão de negócios*, 17:1116–1133, 2015.

[111] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[112] Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, pages 75–105, 2004.

[113] Vijay K Vaishnavi and William Kuechler. *Design science research methods and patterns: innovating information and communication technology*. Crc Press, 2015.

[114] John Mingers. Combining is research methods: towards a pluralist methodology. *Information systems research*, 12(3):240–259, 2001.

[115] Hannah Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104:333–339, 2019.

[116] Lifeng Ren, Yanqiong Zhang, Yiren Wang, and Zhenqiu Sun. Comparative analysis of a novel m-topsis method and topsis. *Applied Mathematics Research eXpress*, 2007, 2007.

[117] Fatma Dammak, Leila Baccour, and Adel M Alimi. Crisp multi-criteria decision making methods: State of the art. *International Journal of Computer Science and Information Security*, 14(8):252, 2016.

[118] Jose Sanchez, Raphael Caire, and Nouredine Hadjsaid. Ict and electric power systems interdependencies modeling. In *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, pages 1–6. VDE, 2013.

[119] Wolfgang Borutzky. *Bond graph methodology: development and analysis of multidisciplinary dynamic system models*. Springer Science & Business Media, 2009.

[120] Paulo Carreira, Vasco Amaral, and Hans Vangheluwe. *Foundations of multi-paradigm modelling for cyber-physical systems*. Springer Nature, 2020.

[121] Georgios Kavallieratos and Sokratis Katsikas. Attack path analysis for cyber physical systems. In *Computer Security*, pages 19–33. Springer, 2020.

[122] Nicolas Pelissero, Pedro Merino Laso, and John Puentes. Model graph generation for naval cyber-physical systems. In *OCEANS 2021: San Diego–Porto*, pages 1–5. IEEE, 2021.

[123] M Midhun and Manjula Devananda. Veterinary medication prescription analysis: A machine learning approach. In *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, pages 1–6. IEEE, 2022.

[124] Adam Szekeres and Einar Snekkenes. Representing decision-makers in sgam-h: the smart grid architecture model extended with the human layer. In *International Workshop on Graphical Models for Security*, pages 87–110. Springer, 2020.

[125] Esmaeil Atashpaz-Gargari and Caro Lucas. Imperialist competitive algorithm: an algorithm for optimization inspired by imperialistic competition. In *2007 IEEE congress on evolutionary computation*, pages 4661–4667. Ieee, 2007.

Part II: Research Articles

7 Article I: Cyber-Physical Interdependencies in Power Plant systems: A Review of Cyber Security Risks [2]

This article is not included due to copyright
Available at IEEE Xplore
https:/doi.org/10.1109CICT48419.2019.9066188

8 Article II: Identifying Critical Components in Large Scale Cyber Physical Systems [3]

https://doi.org/10.1145/3387940.3391473

9 Article III: Identifying and Analyzing Dependencies in and among Complex Cyber Physical Systems [4]

sensors

Article

Identifying and Analyzing Dependencies in and among Complex Cyber Physical Systems

Aida Akbarzadeh * and Sokratis Katsikas

Department of Information Security and Communication Technology, Norwegian University of Science and Technology , N-2815 Gjøvik, Norway; sokratis.katsikas@ntnu.no
* Correspondence: aida.akbarzadeh@ntnu.no

Abstract: Contemporary Critical Infrastructures (CIs), such as the power grid, comprise cyber physical systems that are tightly coupled, to form a complex system of interconnected components with interacting dependencies. Modelling methodologies have been suggested as proper tools to provide better insight into the dependencies and behavioural characteristics of these complex systems. In order to facilitate the study of interconnections in and among critical infrastructures, and to provide a clear view of the interdependencies among their cyber and physical components, this paper proposes a novel method, based on a graphical model called Modified Dependency Structure Matrix (MDSM). The MDSM provides a compact perspective of both inter-dependency and intra-dependency between subsystems of one complex system or two distinct systems. Additionally, we propose four parameters that allow the quantitative assessment of the characteristics of dependencies, including multi-order dependencies in large scale CIs. We illustrate the workings of the proposed method by applying it to a micro-distribution network based on the G2ELAB 14-Bus model. The results provide valuable insight into the dependencies among the network components and substantiate the applicability of the proposed method for analyzing large scale cyber physical systems.

Keywords: cyber physical systems; system of systems; graph theory; multi-order dependencies; cybersecurity

check for updates

Citation: Akbarzadeh, A.; Katsikas, S. Identifying and Analyzing Dependencies in and among Complex Cyber Physical Systems. *Sensors* **2021**, *21*, 1685. https://doi.org/10.3390/s21051685

Academic Editor: Panagiotis Sarigiannidis

Received: 8 February 2021
Accepted: 22 February 2021
Published: 1 March 2021

1. Introduction

With the rapid growth of merging Information and Communication Technology (ICT) with Critical Infrastructures (CIs) such as Energy and Transportation systems, the complexity of CIs drastically increased and Cyber–Physical Systems (CPSs) have been formed. CPSs are the result of integrating the computing, communication, and control capabilities, with physical processes which were developed to facilitate the monitoring and controlling of system components in the physical world [1]. Although this progress enhanced the efficiency and service coverage of CIs, it significantly increased the connections among the system components as well as the interdependencies between different sectors of CIs, such as the dependency between the transportation system and the power and telecommunication systems.

These intricate dependencies make systems more vulnerable because in this way any failure of critical infrastructure will have a considerable impact not only on the infrastructure itself but also on the other dependent infrastructures. As an example, in 2001 an electric power disruption in California, caused a cascading failure and affected oil and natural gas production, refinery operations, gasoline transportation, key industries and the water and agriculture sectors, which led to major financial loss [2]. Two years later the blackouts in the USA–Canada and Southern Sweden and Eastern Denmark revealed the possibility of international cascading effects. In general, recent blackouts [3] and studies on their impact [4] clearly showed this strong dependency between the electrical infrastructure as an individual CPS and other CIs and the consequences of this dependency.

Meanwhile, the frequency and impact of recent blackouts, particularly in Europe and North America, are progressively growing; this could also be interpreted as a remarkable warning for all CIs [5,6]. The vulnerability of the electrical infrastructure by itself mainly stems from the heterogeneity of connections and dependencies among the system components. This vulnerability has grown after the merging of the electrical infrastructure with information and communication systems and turned electrical infrastructure into an attractive target for cyber attacks. In electrical infrastructure, like other CIs, any individual part and facet of a system has its special characteristics; this affects the behaviour of the entire system when it encounters an unexpected situation such as a cyber or a cyber physical attack [7]. Therefore, detecting the chain of dependency and studying the relationships among components of CIs, particularly inside the electrical infrastructure as vital cyber physical systems, are of great importance for the maintenance of key processes which substantially impact on the economy and societal well being.

Modelling and simulation methods are highly suggested as proper tools to study CPSs. With the main goal of enhancing the resilience and security of complex systems, valuable researches have been conducted for modelling the dependencies of and in such systems; these include Complex Networks Theory/Graph Theory, Petri-Nets [8], Well-Formed Nets (SWN) [9], Input-Output Models [10], Bayesian Networks [11], Matrix representations, Boolean logic Driven Markov Processes (BDMP), Agent-Based Models and Multi-Agent Modelling [12]. Most of the aforementioned studies focus on qualitative or semi-qualitative analyses. Unfortunately, such approaches provide inadequate knowledge to system designers and decision-makers with the responsibility to mitigate negative impacts and to manage risks arising from dependencies inside a system, since operators not only need to know about the connectivity and dependencies, but their magnitude and characteristics as well [13,14].

Despite significant efforts in recent years, analysis and modelling of CPSs is still a challenging problem in basic research on complex systems; because in this context, CPSs are not analysed as discrete assets or services within particular sectors. Instead, a holistic system-of-systems view is followed, in which all the connections between different subsystems and sub-layers of a CPS are considered [15]. Even though Graph Theory-based methods were known as the most common and effective approaches to reveal the hidden dependencies [16], reviews of recent studies show that utilizing Graph Theory to study large scale systems such as electrical infrastructures will result in massive complicated diagrams that cannot be easily understood and cannot assist in distinguishing the impact of dependencies [17]. Nevertheless, graphical models developed based on Graph Theory such as Network Analysis and Design Structure Matrix (DSM) have addressed these issues to some extent and represented promising results to evaluate the characteristics of connections in CPSs. DSM has been mainly developed to extract the interrelationships exist between the activities of a complex design problem to break them down into smaller sub-problems. More precisely, in the DSM, the connectivity between the elements of a system should be represented in the form of a matrix first and then different methods such as clustering will be applied to find probable dependencies or structural patterns that might exist. However, due to the fact that this model requires to analyse of all the system connections to extract probable dependencies, DSM could not be an efficient method to study characteristics of connections in large scale CPSs. To tackle this challenge, we propose MDSM, a modified version of DSM in which the searching based algorithms in the analysis phase of the DSM are replaced with a lightweight and deterministic approach. Indeed, MDSM not only has lower computational complexity but also extracts the characteristics of connections for all the system components and represent the result in a predefined systematic structure, unlike DSM. Moreover, to facilitate the quantitative analysis of dependencies of complex systems, the inter-dependency and the intra-dependency are located in predefined and separate parts in the MDSM.

Indeed, applying a graphical model to represent the interconnections between different subsystems of a large-scale CPS effectively enhances the knowledge about the connectivity within the systems and presents more details on the behaviour of different subsystems while working as a whole, in particular on their interdependencies. Therefore, this paper first attempts to develop a simple yet useful graphical method to represent coupled critical infrastructures to facilitate the identification of dependencies within CIs and then proposes quantitative parameters to evaluate the characteristics of dependencies inside large scale systems in order to enhance the security and robustness. Our main contributions are as follows:

- We propose MDSM as a graphical model to extract characteristics of connections inside a cyber-physical system to facilitate studying the behaviour of dependent components of large scale systems including, both intra-dependency and inter-dependency.
- We propose four quantitative dependency parameters, namely the Impact of Dependency (IoD), the Susceptibility of Dependency (SoD), the Weight of Dependency (WoD) and the Criticality of Dependency (CoD) to measure the characteristics of dependencies.
- We propose a method to aggregate quantitative dependency parameters of the higher order of dependency to evaluate the characteristics of multi-order dependencies in CPSs.
- We illustrate the application of the proposed method to a reduced scale network from a real French Distribution Network with 14 power-bus.

The rest of the paper is organized as follows: In Section 2, we review the related work on modelling dependencies in CIs. Section 3 describes the proposed method, while Section 4 explains the concept of the higher order of dependency in system-of-systems. A case study is presented in Section 5 to evaluate the applicability of the proposed method and application of dependency analysis is expounded in Section 6. Finally, Section 7 summarizes our conclusions and indicates directions for future work.

2. Related Work

As discussed earlier, critical infrastructures depend on each other to operate properly and these expanding connections among them, be they tangible or intangible, have increased the vulnerabilities of CIs. The term dependency refers to a connection or linkage between two components, through which the state of one component influences the state of the other. While interdependency is a two-way dependency, a mutual dependency, between two components such that the state of each component influences or is correlated to the state of the other one.

Exploiting the six dimensions of interdependencies proposed by Rinaldi et al. [2] namely, type of failure, infrastructure characteristics, state of operation, environment, coupling and response behaviour and types of interdependencies, facilitates the identification of interdependencies inside CIs. Each dependency between two components may be represented by modelling the connection between them, which is one of the following types:

- Input, Mutual, Shared, Exclusive, Co-located [18];
- Physical, Cyber, Geographic, Logical [2];
- Functional, Physical, Budgetary, Market and economic [19];
- Physical, Geospatial, Policy, Informational [20].

Ouyang et al. [21] developed ten different scenarios to evaluate these types of dependencies in CIs and concluded that utilising the type of interdependencies proposed by [2] provides better results in terms of covering a variety of scenarios. Nieuwenhuijs et al. [22] asserted that the geographical interdependencies are the result of a common mode failure rather than a type of dependency that was mentioned in [2]. Rinaldi et al. [2] proposed Cascading failure, Escalating failure and Common cause failure as three different types of dependency-related failures as a dimension of dependency. Later, the result of an empirical study indicated that dependency-related failures in systems could be categorized into either cascade-initiating or cascade-resulting [23]. In general, analysing dependencies through this dimension increases the system resilience as it facilitates the identification of failures that might occur in CIs. Such failures can disturb the functionality of systems, thus affecting their reliability. Modelling dependencies of CIs in order to understand the behaviour of complex systems encountered with failures that may be caused by adversaries is a common approach towards enhancing the reliability of systems [24,25]. In general, modelling CIs in terms of their interdependencies provides an insightful view of inter-system and intra-system causal relationships, response behaviour, failure types, state of operation, and risks that arise due to the dependency-related failures in systems [26,27]. Accordingly, significant efforts have been made to develop appropriate models to map out the interdependencies of complex systems. Even though several researchers attempted to model dependencies between all the critical infrastructures [28–30], the majority focused on limited numbers of critical infrastructures [31,32], particularly on the power and ICT infrastructures [33,34].

In fact, large scale blackouts and the ongoing transition towards smart grids and the idea of developing smart cities across the globe decisively highlighted the impact of the power systems on the reliability of all CIs in different sectors [35]. An empirical study on different CIs showed that energy and telecommunications are the main cascading-initiating sectors [23]. As a result, significant efforts have been made in the last few years to study and model the interdependencies of power systems combined with ICT systems, viewed as complex cyber-physical systems, to improve defensive and protective strategies in the cyber and physical layers of power systems [33–37].

Researchers in many domains attempt to identify suitable methods to model real systems, considering the relations and dependencies between the systems' components. Satumtira et al. [38] surveyed 162 papers on interdependency modelling, among which the Graph Theory/Complex Network Theory (at 22% of the studies) was the most common method to study interdependencies in CIs. Input-output models were next, followed by agent-based models that were used in 11% of the studies. Each of these methods has its own advantages and weaknesses in modelling CIs in terms of different dimensions of interdependency. For instance, the input-output model, that is inherently a method to study the economic flow, has been applied recently to calculate economic losses that result from the unavailability of different sectors in CIs and their interdependencies. This model has also been modified in a way that could evaluate the spread of risk among system components [39,40]. Nevertheless, input-output modelling may not be used in holistic approaches to capture both functional and geographic interdependencies [41].

Torres [42] suggested six different objectives namely Scalability, CPU time, Usability, Tools accessibility, Dynamic simulation and Large systems modeling to evaluate different methods including Agent-based Model, Petri Nets, Bayesian Networks, BDMP and Complex Network Theory/Graph Theory for modelling CIs. Comparing those methods by the author revealed that the Complex Network Theory with the highest value in four out of six different objectives has the best results, which confirmed the applicability of this method to model CIs [42]. Indeed, the Complex Network Theory is developed based on the Graph Theory to study real networks in social and computer science, biology, telecommunication, transport, electronics, electrical engineering, and other domains with complex systems [43].

According to Graph Theory, topological analysis allows us to describe the connectivity of complex systems and to model the relationships between system components and their characteristics with less data. The topology-based method facilitates vulnerability assessment and can provide a clear view of the role and importance of each component and connection in the systems, as well as to fully cover all types of interdependencies; no other model has this ability [21,44,45]. Therefore, this method is a suitable choice for analysing complex systems, since it explicitly includes the interactions and dependencies within/between systems and provides a simple yet powerful means to evaluate and manage complex systems architectures [35].

Likewise, derivatives of Graph Theory in the context of the topological analysis, such as matrix-based system modelling representation (Adjacency matrix) and Network Analysis and Design Structure Matrix (DSM) visualize the system components and interactions as graphical nodes and lines [46,47]. This intuitive model reduces the complexity of the analysis process and contributes to improving the understanding of operators [48]. DSM is known as a highly flexible and straightforward modelling technique, which provides valuable insights for engineers and managers in a wide range of fields. This method was initially developed to decompose a complex design problem into sub-problems by displaying the interrelationships between the activities in the form of a matrix. Recently, DSM has been utilized in different fields to study interdependencies; as a result, it is currently referred to as Dependency Structure Matrix Analysis [49]. Eppinger et al. presented the application of DSM in different industries and sectors through 44 practical cases [50]. The growing dependency-related failures within CIs, and the significant impact of CIs on the economy and the quality of life, intensify the necessity of developing modelling methods to study the dependencies and characteristics of complex systems, in particular, for modelling large scale CIs such as power and ICT systems.

DSM represents the interaction among the elements of a system in a square matrix with the inputs in rows and outputs in columns (Figure 1b). Then, based on the type of the system and its application, different analytical methods such as the clustering and sequencing analysis can be applied to extract the relations among the desired elements of the system (Figure 1c). In other words, DSM first documents the relationships among the elements of a system and then utilizes clustering analysis and rearranges the system's elements in order to find structural patterns that might exist in the system, such as an interdependency.

We propose the modified DSM in Section 3 to turn the DSM into a predefined systematic structure for representing interactions between two subsystems without the need for those analytical methods. In this way, not only the computational complexity will decrease, but MDSM will also assist in extracting the characteristics of connections for all the system components, unlike the DSM. In MDSM the direction of connections between components is clearly distinguishable and inter-dependency and intra-dependency are placed in predefined and separate parts; this greatly facilitates further analysis and calculations. We also introduce four dependency parameters to evaluate and analyse the weight, impact and criticality of each dependency relationship between components in a quantitative manner.

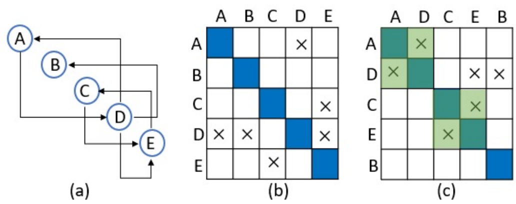


Figure 1. A sample digraph (**a**), its equivalent DSM (**b**) and the result of DSM sequencing which is indicated in green blocks (**c**).

3. Modified Dependency Structure Matrix (MDSM) Method

In this section, the process of forming an MDSM to representing the relationships between two subsystems in a CPS is described, and different characteristics of dependencies within a complex system are extracted from the MDSM. The applicability of the proposed method in large scale CPSs is also explored in more detail. The MDSM method is a graphical approach to demonstrate the dependencies and interdependencies between two subsystems of a CPS. The whole process follows a six-step approach, namely Set up, Modify, Rearrange, Display, Identify and Analyze. The outcome is represented as a square $N \times N$ matrix, in which N contains the elements of both subsystems. Each of these steps is described in the following:

3.1. Set up (Step 1)

The first step of MDSM is to define two domains or subsystems of interest and capture the connections inside each subsystem, as well as between two subsystems. The collected data could simply be mapped as a directed graph D to show elements of each subsystem and their connections, with the direction being preserved. In Graph Theory, a directed graph or in short form digraph D is a pair (V, A) where V is a set of vertices (nodes) and A is a subset of $V \times V \equiv \{(x, x)|x \in V\}$ called arcs. If $(u, v) \in A$ then the arc $a = \langle \overrightarrow{u, vs.} \rangle$ joins the initial vertex (tail) u to its terminal vertex (head) v [51].

Once the essential data are collected, we use the adjacency (or connectivity) matrix A of order N, where N denotes the total number of nodes, to represent the result. Rows and columns of matrix A are labeled according to the total number of elements while grouped into subsystems, and each row and its corresponding column in A is filled out taking into account the direction of the connection. A is a binary matrix and each nonzero value in row i column j indicates an arc $\langle \overrightarrow{i, j} \rangle$ which means that node j depends upon node i.

Without loss of generality and for the sake of clarity, suppose that we want to apply MDSM to study the dependency characteristics and connectivity properties of a smart grid system, a power-communication network that comprises both power and communication components, and that the two subsystems of interest are the Power system (Physical) and the Communication system (Cyber). Subsequently, first we need to collect the topological data of all nodes in the physical part $V_p \equiv \{v_1, v_2, ..., v_p\}$, and the cyber part $V_c \equiv \{v_1, v_2, ..., v_c\}$. Then, the matrix A of order $N = (p + c)$ is set up to illustrate the relationship between each pair of nodes as follows:

$$A_{N,N} = \begin{pmatrix} a_{p_1p_1} & \cdots & a_{p_1p_p} & a_{p_1c_1} & \cdots & a_{p_1c_c} \\ \vdots & ... & \vdots & \vdots & ... & \vdots \\ a_{p_pp_1} & \cdots & a_{p_pp_p} & a_{p_pc_1} & \cdots & a_{p_pc_c} \\ a_{c_1p_1} & \cdots & a_{c_1p_p} & a_{c_1c_1} & \cdots & a_{c_1c_c} \\ \vdots & ... & \vdots & \vdots & ... & \vdots \\ a_{c_cp_1} & \cdots & a_{c_cp_p} & a_{c_cc_1} & \cdots & a_{c_cc_c} \end{pmatrix}$$

3.2. Modify (Step 2)

To date, all the connections related to subsystems have been laid out in matrix A. As mentioned earlier, each nonzero element in matrix A shows a connection between corresponding nodes while preserving the direction of the connection. However, a closer look at the indices assigned to each element of matrix A reveals that A consists of four distinct parts, each one of which denotes a particular type of relationship, as shown in the following equations:

$$Type1 : \Big\{ a(i, j)|i \in V_p, \quad j \in V_p \tag{1}$$

$$Type2 : \Big\{ a(i, j)|i \in V_c, \quad j \in V_c \tag{2}$$

$$Type3 : \Big\{ a(i, j)|i \in V_p, \quad j \in V_c \tag{3}$$

$$Type4 : \Big\{ a(i, j)|i \in V_c, \quad j \in V_p \tag{4}$$

Equations (1) and (2) point to an intra-dependency, where two nodes from the same subsystem are connected. On the other hand, linking two different types of nodes as in Equations (3) and (4), forms an inter-dependency between two subsystems and, it means that the performance of one node in the host subsystem depends on one node from another subsystem. Although various types of dependency within subsystems are identified in the matrix A, yet its distributed pattern caused these data to remain elusive so far. To address this challenge, we apply a systematic approach based on the general concept of DSM [50] to modify the current structure of nodes in a way that the salient connectivity properties of each node could be identified and utilized in further processing.

We use complex numbers to distinguish between different types of dependencies. All the nonzero elements of Type 2 and Type 4 in matrix A turn to imaginary, i.e., 1 is represented as i. Then, all the elements of Type 3 transpose and merge with the elements of Type 4. The new structure, called MDSM, is as follows:

$$MDSM = \begin{pmatrix} a_{p_1p_1} & \dots & a_{p_1p_p} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{p_pp_1} & \dots & a_{p_pp_p} & 0 & \dots & 0 \\ a_{p_1c_1} + ia_{c_1p_1} & \dots & a_{p_pc_1} + ia_{c_1p_p} & ia_{c_1c_1} & \dots & ia_{c_1c_c} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{p_1c_c} + ia_{c_cp_1} & \dots & a_{p_pc_c} + i_{c_cp_p} & ia_{c_cc_1} & \dots & ia_{c_cc_c} \end{pmatrix}$$

Modifying the structure of matrix A provides clear and meaningful insight into the interactions among system components while decreases the complexity. Having the MDSM, one can easily access to different types of dependency in predefined spots that will facilitate further study and computations.

3.3. Rearrange (Step 3)

This step aims to represent a compact view of the system interactions by decreasing the distance between nonzero elements of the MDSM while preserving the system topology.

Recent studies discovered that most of the complex systems like CIs have a scale-free characteristic [52]. These systems, particularly the power and communication systems, have less redundant links; this means that the graph representing such systems will be sparse (a graph $G = (V, A)$ is sparse if $|A|$ is much smaller than $|V|^2$), and consequently the resulting matrix A for such systems will, in general, be sparse [53]. Table 1 is an example of this sparsity which compares the number of links and nodes in several standard IEEE test systems. Imagine that we want to demonstrate connections among the 118 components of the IEEE 118-Bus (without considering the second subsystem). The adjacency matrix of this system is a 118×118 matrix, in which only 179 elements out of the total 13924 elements are nonzero. This means that a large number of elements in a 118×118 matrix that are spread in the matrix A should be examined to analyse the connection properties, even though only 1.3 % of the elements are nonzero.

Table 1. Number of links and nodes in IEEE test systems.

System	N.Nodes	N.Links
IEEE 9-Bus	9	9
IEEE 14-Bus	14	20
IEEE 24-Bus	24	34
IEEE 39-Bus	39	46
IEEE 118-Bus	118	179

MDSM has been designed to facilitate the analysis of connection properties and in particular, the identification of characteristics of dependency in large scale CPSs. To this end, minimization of the distance between nonzero elements of the MDSM will enhance the efficiency of the method, will provide better visualization, and will reduce the computational complexity of mathematical methods that can leverage the MDSM; such minimization can be achieved by appropriately reordering the columns of the MDSM. These columns will be moved with their labels to preserve the system topology. However, reordering the columns of MDSM to decrease the distance between the nonzero elements of one row could increase the distance between the nonzero elements of the other rows. Besides, there might be different permutations that lead to similar, as regards the optimality criterion, results. Thus, an optimization algorithm is required to compute the global optimum for rearranging the MDSM.

Several algorithms have been proposed during the last two decades to solve optimization problems in different domains, such as the Genetic Algorithm (GA) [54], the Simulated

Annealing (SA) [55], the Ant Colony Optimization (ACO) [56] and the Imperialist Competitive Algorithm (ICA) [57]. Among them ICA, which was developed based on the swarm intelligence theory by Atashpaz et.al [57], has been widely applied to address different optimization problems in engineering, scheduling, data clustering, network flows, facility layout and neural networks, to name a few [58]. In [58] the superiority of ICA as compared to other evolutionary algorithms, in particular regarding its flexibility, robustness, reasonable computational time, scalability and ability to handle a large number of decision variables was established. These characteristics, as well as the wide range of problems that have been solved by ICA in engineering, make the ICA an ideal choice to apply in the Rearrange step of our proposed method. In the sequel, we describe how ICA can be used to address the MDSM columns reordering problem.

ICA begins with an initial population; each individual of this population is called a country. Then, some of the best countries (with the least cost) are labelled as imperialists, and the rest of them will be the colonies of these imperialists. In our case, each country represents one possible permutation of columns in the MDSM. For each country, the cost is defined as the sum of the absolute distance between every two nonzero adjacent elements in all rows of MDSM. This is computed by means of the Cost Function, the pseudo code of which is shown in Algorithm 1.

Algorithm 1 (Cost Function).

```
1: for i = 1 to N_row do
2:     Find the column index of non-zero elements in row i and store in the vector P;
3:     for k = 1 to Numel(P) − 1 do
4:         Compute the CostFunction = P_k − P_{k+1};
5:     end for
6: end for
```

Based on the power of the imperialists, which is inversely proportional to the cost, all the colonies are divided among the imperialists and each imperialist together with its colonies form an empire. After that, according to the two main operators, Assimilation and Revolution, colonies start moving toward their relevant imperialist and the Intra-Empire Competition starts. In case the power of a colony exceeds the power of the associated imperialist inside the same empire, that colony and the imperialist swap roles. Then the Inter-Empire Competition begins, in which the weakest empire loses its weakest colony and thereby its power decreases, while the winner of the inter-empire competition will possess that colony and in consequence gain more power. The power of each empire is computed based on a linear combination of the imperialist' power and the mean power of its relevant colonies in the empire. Through the imperialistic competition, the powerful empires will gradually grow and gain more power. The result of this process identifies the optimum permutation for reordering the columns of MDSM.

Rearranging the columns of a sparse MDSM using ICA will increase the efficiency of further computations, and will provide a better display. Additionally, the proposed method could be also applied to other domains and systems with dense connections. In this case, step 3 (discussed in Section 3.3) could be skipped without affecting the final result.

3.4. Display (Step 4)

The ICA will identify the optimum permutation of columns in MDSM in polynomial-time and will show it as a vector of size p, where p denotes the number of elements in the first subsystem (physical) under study. According to this vector, the columns of MDSM are rearranged and the MDSM is updated. The new structured arrangement of elements and interactions in MDSM provides an appropriate compact representation for complex CPSs. In comparison with previous network modelling approaches such as those utilizing graph and adjacency matrix, MDSM can extract meaningful relations among components of a large scale system and represent it in a predefined and relatively small space.

To demonstrate the structure of MDSM a small scale sample of MDSM is presented in Figure 2, which reflects the relationships between two subsystems of order $p \times c$. As illustrated in Figure 2, MDSM categorised connections into three parts. The green part displays the inter-dependency between two subsystems which we call it the "inter-dependency part", while the blue and the orange parts, named as "intra-dependency part", refer to the connections inside the first subsystem and the second subsystem, respectively.

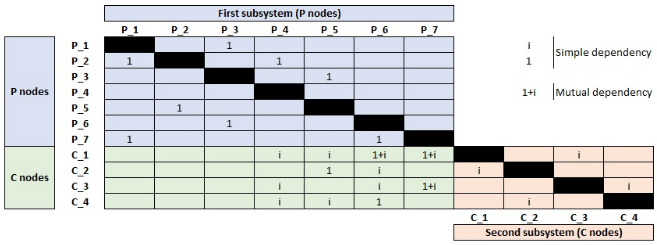


Figure 2. MDSM.

3.5. Identify (Step 5)

Once the MDSM is displayed, characteristics of a complex system could be simply observed, and relationships among the components become apparent from even a cursory review. The MDSM particularly highlights the dependency patterns that could be divided into dependency (i.e., simple dependency) and interdependency (i.e., mutual dependency) as shown in Figure 3.

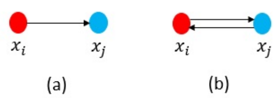


Figure 3. (**a**) Dependency (simple dependency) and (**b**) Interdependency (mutual dependency).

Dependency is demonstrated by 1 or *i* in the MDSM and shows that one component in a subsystem depends on another component, either from the same or the other subsystem (Figure 2). However, interdependency is a bidirectional path between two components belong to two different subsystems $V \times V \equiv \{(x_i, x_j)|x_i \in Vp \ \& \ x_j \in Vc\}$, and indicates the presence of two paths, i.e., $x_i \to x_j$ and $x_j \to x_i$ in the directed graph of the system which means that x_i and x_j depend on each other. This is displayed as a complex number $i + 1$ in the inter-dependency part of the MDSM in Figure 2 and shows that in a CPS, one can have access from the first subsystem (i.e., physical layer) to the second subsystem (i.e., cyber layer) and vice versa. When two systems are connected, the new compound system could be more fragile than each of its constituents as unforeseen dependencies between two systems can be targeted by attackers, or a simple failure in one part may lead to cascading failures in the entire system. For instance, attackers might leverage a dependency link between two systems as an infiltration point to make an attack path into the other system (see Figure 4). Therefore, dependency and interdependency in the inter-dependency part of an MDSM could be considered as jumping points between subsystems, and analysis of these points could play important role in mitigating risks and enhancing security and safety in CPSs.

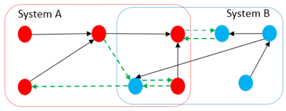


Figure 4. The green dashed edges represent the dependency within a complex system.

3.6. *Analyze (Step 6)*

The identification of different types of dependency, and more precisely in the inter-dependency part of the MDSM, in step 5 provides the essential requirements for quantitative analysis of the criticality and the impact of each dependency between two subsystems. Dependencies between two subsystems could affect the behaviour of a whole CPS as a system-of-systems in different ways and might cause undesired consequences. For these reasons, by utilizing the proposed inter-dependency part of the MDSM we scrutinize these different aspects and develop quantitative parameters to evaluate the effect of dependencies on the operability of the entire system. Considering the parameters proposed in [59], we define four parameters to study the characteristics of the dependent components between two subsystems, namely Impact of Dependency (IoD), Susceptibility of Dependency (SoD), Weight of Dependency (WoD) and Criticality of Dependency (CoD). We also present the concept of the higher order of dependency based on the proposed parameters to evaluate the chain of dependencies in systems. The proposed parameters are defined in the following paragraphs.

3.6.1. Impact of Dependency (IoD)

In the MDSM, IoD determines the impact of one particular node x_i on the components of another subsystem under study, by measuring the number of components that are influenced by that node (x_i). IoD_{Inter} shows how many components in a subsystem depend on the functionality of a single node in another subsystem. In other words, it measures the potential power of a node to affect another subsystem.

Based on the MDSM, it is also possible to measure the impact of each node within the system it belongs to with IoD_{Intra}. However, our emphasis here is mainly on the analysis of the interactions between two subsystems and corresponding consequences.

To compute the IoD_{Inter} of the ith node from the first subsystem (i.e., p_i), one needs to count how many times the real number "1" is shown in the ith column of the inter-dependency part in the MDSM. Equation 5 shows how this parameter is measured.

$$IoD_{Inter}(p_i) = \sum_{j=1}^{c} Re(p_i, c_j) \tag{5}$$

IoD_{Intra} of the ith node from the first subsystem (i.e., p_i) counts how many times the real number "1" is shown in the ith row of the intra-dependency part of the first subsystem in the MDSM (Equation (6)).

$$IoD_{Intra}(p_i) = \sum_{j=1}^{p} Re(p_i, p_j) \tag{6}$$

For each node of the second subsystem (i.e., c_i), the values of $IoD_{Inter}(c_i)$ and $IoD_{Intra}(c_i)$ are computed by counting the instances of the imaginary number "i" in the ith row of the inter-dependency part and the intra-dependency part of the second subsystem in the MDSM, respectively.

$$IoD_{Inter}(c_i) = \sum_{j=1}^{p} Im(c_i, p_j) \tag{7}$$

$$IoD_{Intra}(c_i) = \sum_{j=1}^{c} Im(c_i, c_j) \quad (8)$$

Notice that (p_i, c_j) indicates the directed path from p_i to c_j, while (c_i, p_j) refers to the directed path $c_i \rightarrow p_j$. For instance, the IoD_{Inter} of the first element in the second subsystem (i.e., $IoD_{Inter}(c_1)$), in Figure 2 equals to 4, since c_1 has access to four elements of the first subsystem. Likewise, the value of IoD_{Inter} of P_6 is equal to 2, i.e., $IoD_{Inter}(p_6) = 2$.

In general, nodes with a higher value of IoD have more impact on the system. For instance, in Figure 5a, if node x_1 fails, only one node y_1 fails too. However, in Figure 5b three nodes $\{y_1, y_2, y_3\}$ will stop working, by the x_2 failure.

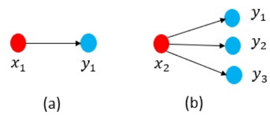


Figure 5. Impact of dependency; (**a**) $IoD_{x_1} = 1$ and (**b**) $IoD_{x_2} = 3$.

3.6.2. Susceptibility of Dependency (SoD)

Susceptibility of dependency shows how much the operability of one node in a subsystem is depending on the operability of other nodes in another subsystem. For each component in a subsystem, the more links a node receives, the higher level of susceptibility it has.

Assume that we are interested in computing the SoD_{Inter} of p_j from the first subsystem. According to the inter-dependency part of the MDSM, we simply need to count the number of links incident upon p_j from the second subsystem, which is represented by the imaginary number "i" (see Equation (9)).

$$SoD_{Inter}(p_j) = \sum_{i=1}^{c} Im(c_i, p_j) \quad (9)$$

As shown in Equation (10), SoD_{Intra} of the jth node from the first subsystem (i.e., p_j) counts how many times the real number "1" is shown in the jth column of the intra-dependency part of the first subsystem in the MDSM.

$$SoD_{Intra}(p_j) = \sum_{i=1}^{p} Re(p_i, p_j) \quad (10)$$

Likewise, for those nodes that belong to the second subsystem in the MDSM (i.e., c_j), the $SoD_{Inter}(c_j)$ and $SoD_{Intra}(c_j)$ is calculated based on the following equations:

$$SoD_{Inter}(c_j) = \sum_{i=1}^{p} Re(p_i, c_j) \quad (11)$$

$$SoD_{Intra}(c_j) = \sum_{i=1}^{c} Im(c_i, c_j) \quad (12)$$

As an example, the SoD_{Inter} of p_6 in Figure 2, is equal to 3, because three links from $\{c_1, c_2, c_3\}$ towards p_6 exist. In line with Equation (11), the value of $SoD_{Inter}(c_1)$ in Figure 2, is equal to 2 (i.e., $SoD_{Inter}(c_1) = 2$).

Indeed, the susceptibility of dependency is a useful parameter from both the defender and attacker point of view. For example, suppose that an attacker tends to target a highly protected node x_1 in Figure 6. Due to the cost of the attack, the attacker may alternatively attempt to target node x_1 through the x_1's neighbour nodes. In this case, with reference to Figure 6b the attacker could influence node x_1 either through y_1 or y_2. However, in Figure 6a there is only one option. As mentioned earlier, the more links a node receives, the higher level of susceptibility it has. This parameter could be applied to investigate attack surfaces in complex systems as well as to analyse and predict probable attack paths.

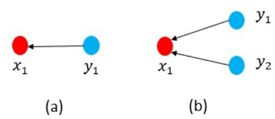


Figure 6. Susceptibility of dependency; (**a**) $SoD_{x_1} = 1$ and (**b**) $SoD_{x_1} = 2$.

3.6.3. Weight of Dependency (WoD)

In general, SoD and IoD measure that how many components in a system are affected by or impacted on other components because of the presence of a dependency in a system. However, the strength of dependency differs with its type. An interdependency in a system has a higher impact compared to a dependency. That is because if a node at one end of an interdependency fails or one of the mutual dependency links stop working, the corresponding node at the other end might not act properly, and the response would not be sent via the other link, i.e., the other link will also fail.

An interdependency has the potential of making common cause failure or even cascading failures to form a closed-loop in the system, which can continuously oscillate the values and states of the connected components. This would be more clear from the security perspective.

Accordingly, the weight of dependency which is assigned to an interdependency is α times greater than that of a dependency. Parameter α is defined as a power of 2, $\alpha = 2^n$, in which n could be adjusted based on the importance of interdependencies for specific purposes and domains, but in general, it is defined as follows:

$$\begin{aligned} \text{(Dependency)} \quad &: \quad n = 0 \rightarrow \alpha = 1 \\ \text{(Interdependency)} &: \quad n = 1 \rightarrow \alpha = 2 \end{aligned}$$

3.6.4. Criticality of Dependency (CoD)

Each system or subsystem consists of several components whose functionality highly affects the performance of the entire system; these are known as the critical components. To enhance the reliability of systems, we always try to keep the critical components away from any failures or unsecured connections and various methods have been proposed to identify critical components. However, once these components are identified within a system, it is still essential to protect them from potential vulnerabilities that might arise as a consequence of connecting new components or subsystems to the main system. It is precisely at this point that MDSM could be of great aid in modelling connections of a system-of-systems, and provide a clear view of these critical components in terms of connectivity. Based on that, Criticality of Dependency (CoD) measures how close a critical component from one subsystem is to components of the other subsystem. The CoD along with other proposed parameters, SoD, IoD and WoD, will help one to study the properties of dependency links in a system-of-systems and investigate whether these connections might threaten the critical components of the system and increase the risk.

In the following examples, we measure the first order of the CoD which shows whether there is a direct connection between a component in one subsystem and a critical component in another subsystem, or not. Imagine that c_1 is identified as the critical node of the second subsystem in Figure 2. Then, because of the connection between $\{p_6, p_7\}$ in the first subsystem with $\{c_1\}$, the CoD of these two components are not zero, which means $CoD_{P_6} = 1$ and $CoD_{p_7} = 1$.

Depending on the level of the accuracy needed to determine the CoD in a system, it is also possible to consider the value of criticality of components in a system instead of having a binary view. Now for a non-binary example, suppose that c_1 and c_3 are both critical nodes of the second subsystem and it has been defined that the role of c_1 is three times more vital than c_3. In this case, the CoD_{p_6} and CoD_{p_7} would be determined as 3 and 4, respectively.

The parameter CoD along with other proposed parameters, SoD, IoD and WoD, will help one to study the properties of dependency links in a system-of-systems and investigate whether these connections might threaten the critical components of the system and increase the risk. In summary, parameters SoD and IoD not only detect the dependent links between subsystems, but also help to evaluate the importance and the impact of those links when compromised, while CoD and WoD describe the properties of each dependency.

4. Higher Order of Dependency in System-of-Systems

As discussed earlier, coupling different systems and infrastructures might increase the vulnerability, as one failure in a system could lead to another failure in the other system and this process could continue back and forth until all connected components, and subsystems fail. Recent blackouts in the US [2], and Italy [60] and their severe impacts are concrete examples of such a cross-sectoral cascading failure in the interconnected infrastructures. These power outages and similar crises in recent years have raised many questions regarding the effect of different types of connections, and the impact of systems rewiring in improving the resilience of the interdependent infrastructures.

In Section 3, four parameters were introduced to extract different characteristics of connections in CPSs. Nevertheless, evaluation of the multi-order of dependency in such interconnected systems could provide a more precise picture of interactions, dependencies, and cascading effects. For these reasons, we define the Higher order dependency (HoD) as a parameter to analyse a system not only based on the direct interactions, but also by considering the chain of dependencies, the impact of the structure of systems, and the effect of all the components in complex systems. To further improve the depth of analysis, HoD could be applied along with the other parameters of dependency. To define the concept of higher order dependency we use the terminology of Graph Theory in [61]. In the directed graph D, for all integer p, $N_D^p(x_i)$ denotes the pth out-neighbourhood node x_i. For instance, if node x_i has a direct connection with nodes $\{x_j, x_k\}$, then the first out-neighbourhood x_i is defined as $N_D^1(x_i) = \{x_j, x_k\}$. Furthermore, if node x_j is connected to x_l, the second out-neighbourhood node x_i will be $N_D^2(x_i) = \{x_l\}$. Indeed, the pth out-neighbourhood of one node represents the pth order of dependency for that node. The higher order of dependency for node x_i is determined as follows:

$x_i \to x_k|$ (First Order)

$x_i \to x_j \to x_l|$ (Second Order)

where the first order of the chain of dependency for x_i includes two nodes $\{x_j, x_k\}$ and the second order only has one node $\{x_l\}$.

The Breadth-First Search (BFS) is an algorithm that could be applied to extract the higher order of dependency. The BFS explores and extracts all the neighbour nodes of each node in a system. In the worst-case, the time complexity of this algorithm is $O(|V + A|)$ and the required space for saving the result is $O(|V|)$ [61]. Based on the level we wish to explore the order of dependency in a system, the time complexity of applying this algorithm to extract the chain of dependencies varies, but in the worst case will be $O(|V + A|)$. Note that V and A are the numbers of nodes and links in a system, respectively.

One approach to compute the value of the HoD is to add together the value of each order. In this case, each order of dependency in the chain of dependency with the length n has the same impact. However, the effect of dependencies in a system tends to decrease with an increase in distance [26]. This will be further explained with the case study in Section 5.

Kotzanikolaou et al. [26] utilized multi-order dependencies to investigate the effect of disruption to interconnected infrastructures. They proposed an equation to compute the cumulative dependency risk based on likelihood and impact considering the chain of dependency among different systems. Here we modify their equation to compute the nth-order of dependency without considering the concept of risk. Let $Y_0 \rightarrow Y_1 \rightarrow ... \rightarrow Y_n$ be a chain of dependency of length n. Then, according to [26], the nth-order of outgoing dependency of Y_0, denoted as $D^n_{Y_0}$, is computed by:

$$D^n_{Y_0} = \sum_{i=1}^{n} (\prod_{j=1}^{i} D_{Y_{j-1},Y_j}) \quad (13)$$

where D_{Y_{j-1},Y_j} is a link between two elements, Y_{j-1} and Y_j. For example, based on Equation (13), the 3rd-order of outgoing dependency of Y_0 is computed as: $D^3_{Y_0} = D_{Y_0,Y_1} + D_{Y_0,Y_1}.D_{Y_1,Y_2} + D_{Y_0,Y_1}.D_{Y_1,Y_2}.D_{Y_2,Y_3}$. Here, the term $D_{Y_0,Y_1}.D_{Y_1,Y_2}$ denotes that Y_0 is connected to Y_2 through the two links D_{Y_0,Y_1} and D_{Y_1,Y_2}. Therefore, considering the Equation (13), multi-order dependencies for each element comprise n times of the first order of dependency, $n-1$ times of the second order of dependency and so on. For simplicity, we can rewrite Equation (13) as follows:

$$HoD_{x_i} = nN^1_D(x_i) + (n-1)N^2_D(x_i) + ... + N^n_D(x_i) \quad (14)$$

Here, n defines the order of dependency. Equation (14) can be applied in different cases to measure the risk, impact and susceptibility by considering the chain of dependency. Unlike [26], all the feedback loops between two subsystems are considered in our study as those are part of the system structure. We will apply the higher order dependency and will discuss the result in Section 5.

5. Case Study

In this section, we analyse the proposed dependency parameters based on the micro-distribution network that was developed on the basis of a real French distribution network with 14 power-bus, called G2ELAB 14-Bus. This system includes both Electric Power System (EPS) and the ICT system (see Figure 7), and has been broadly used in related studies [33,62,63]. Although the advantages of MDSM as a graphical model could be recognized better in large scale systems, this system has been chosen for educational purposes and for allowing the comparison of our results with those in previous works.

In the test system, the EPS (first subsystem) includes 14 power buses, 7 distributed generation sources, 17 lines, 9 loads, and 3 transformers HV/MV and the ICT system (second subsystem) consists of 1 Wimax BS, 5 multiplexers, 3 routers [33,62]. For the sake of simplicity, the digraph of this system is shown in Figure 8, where red circles represent the electrical nodes that belong to the physical part (first subsystem) and nodes of the cyber part (second subsystem) are depicted in blue colour.

Sanchez et al. [62] modelled this system as undirected and directed graphs and measured the Betweenness Centrality and Efficiency of nodes for both perspectives to identify the system vulnerabilities. Later, Milanovic et al. [33] followed the same approach and modelled the system as unidirectional and bidirectional graphs to compute the Node Degree and Efficiency of different types of connections (see Equations (1)–(4) in Section 3) by utilizing complex numbers. The authors also proposed a three-dimensional interconnected model to represent the connections between interconnected ICT and EPS. However, to show the interaction between the two interconnected systems, their model needs two separate matrices. Besides, they asserted that owing to assigning different values such as 1, i, and 1+i to each type of connections in the system, the computational complexity of the method is relatively high. On the contrary, our proposed MDSM can be applied to modelling unidirectional graphs, bidirectional graphs as well as complex systems with hybrid graphs. Moreover, the usage of complex numbers in MDSM is quite different from previous works. In a nutshell, all of those linkages $a = \langle u, \overrightarrow{vs.} \rangle$, either inter-dependency or intra-dependency, which originated from the second subsystem are shown with i, while different types of dependency are recognized based on their predefined position in MDSM.

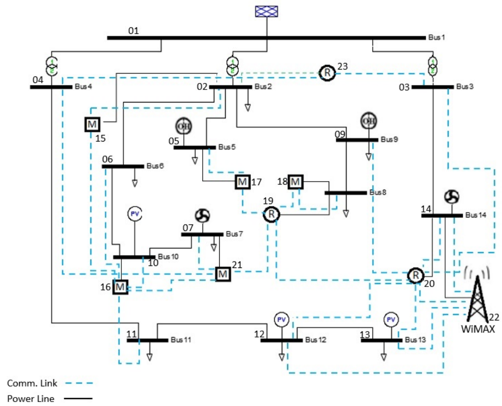


Figure 7. Network structure extracted from a real French distribution network, G2ELAB 14-Bus [33].

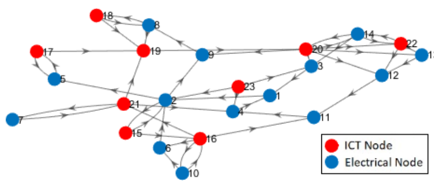


Figure 8. Digraph of the test system.

Based on the topological data of the system, we first construct the MDSM and utilize its dependency part to compute the dependency parameters. The digraph of the dependency part is also depicted in Figure 9 to facilitate the understanding of the interdependency and of the closed-loops that exist between the two subsystems.

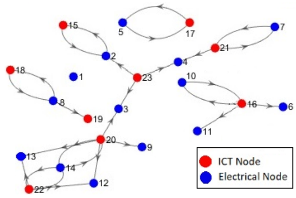


Figure 9. Digraph of the dependency part in MDSM of the test system.

Milanovic et al. [33] argued that the importance of each node in a system can be measured by means of the node degree. Therefore, they computed the node degree of the ICT and EPS components of the test system and concluded that nodes $\{2, 14, 16, 19, 20\}$ are the most important ones. Unlike previous works, the degree distribution of each node in our proposed method is divided into four distinct parts, $\{SoD_{Inter}, SoD_{Intra}, IoD_{Inter}, IoD_{Intra}\}$, which helps to identify the characteristics of each connection and the role of the corresponding nodes in a system. In our method, the total SoD (i.e., $SoD_{Inter} + SoD_{Intra}$) and the total IoD (i.e., $IoD_{Inter} + IoD_{Intra}$) of each node indicates the total number of its inbound and outbound links. Adding these two parameters, the total SoD and the total IoD is equal to the node degree. Figure 10 shows the node degree of each node in the test system.

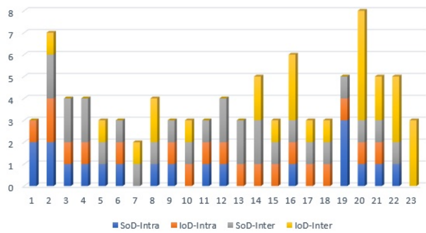


Figure 10. Node degree of the test system: $\{SoD_{Inter} + SoD_{Intra} + IoD_{Inter} + IoD_{Intra}\}$.

Nodes 2 and 19 were identified as remarkable nodes in terms of node degree by the authors in [33], which complies with the values shown in Figure 10. However, referring to the values of $\{SoD_{Inter}, SoD_{Intra}, IoD_{Inter}, IoD_{Intra}\}$ in Figure 10, nodes 2 and 19 are mainly important nodes in their own subsystems, not in the interaction between two subsystems. To make it more clear, Figure 11 depicts SoD_{Inter} and IoD_{Inter} of the test system and reveals that indeed nodes $\{14, 16, 20, 22\}$ play significant roles in the interaction between two subsystems. In contrast to previous works, our proposed parameters can be applied to distinguish between the attributes of dependencies within a complex system, and between the subsystems of a complex system to identify hidden impacts and vulnerabilities.

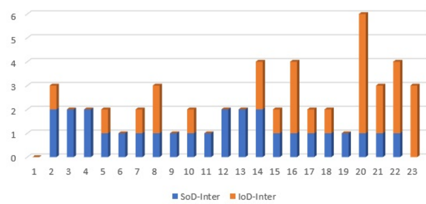


Figure 11. SoD_{Inter} and IoD_{Inter} of the test system.

The values of SoD_{Inter} and IoD_{Inter} of the test system provide more details of the system connectivity. For instance, for all nodes $\{5, 7, 10, 14, 15, 17, 18\}$ in Figure 11, the value of SoD_{Inter} is equal to the value of IoD_{Inter}. In other words, the number of inbound and outbound links of each of those nodes is the same. This might be a sign of closed-loop/interdependency in the system, as we know that for interdependency between two nodes, if those nodes are isolated, each node has the same number of inbound and outbound links. However, in complex systems, one cannot simply rely on the value of SoD_{Inter} and IoD_{Inter} to identify the interdependencies or closed-loops; one would need more information on the properties of connections.

As explained in Section 3, WoD can be applied to measure and to reflect on the properties of dependencies. To this end, the corresponding value of each link based on its type of dependency is taken into account to compute the values of IoD_{Inter} and SoD_{Inter} of each node. The Weight of Dependency of IoD_{Inter} and SoD_{Inter} of the test system is computed and illustrated in Figure 12. Based on Figure 12, measured values of the WoD confirm that each of the nodes $\{5, 7, 10, 14, 15, 17, 18\}$ is part of a closed-loop. Furthermore, to be more specific, these are the end users in closed-loops, which means that these nodes have no other incoming or outgoing links connected. As an example, based on Figure 11 node 7 has two links, and the WoD of each link in Figure 12 is equal to 2, which clearly shows that node 7 has an interdependency.

Apart from interdependencies, the values of the SoD_{Inter}, IoD_{Inter} and the corresponding WoD of each node can be applied to extract the properties of the system connections. For instance, suppose that we wish to analyse the type of dependency of node 22, in the interaction between two subsystems. According to Figure 11, $SoD_{Inter}(22) = 1$ and $IoD_{Inter}(22) = 3$, and Figure 12 shows that $WoD(SoD_{Inter}(22)) = 2$ and $WoD(IoD_{Inter}(22)) = 4$. Referring to Section 3, we showed that the value of WoD for an interdependency is equal to 2. Here the weight of dependency for one single link $SoD_{Inter}(22)$ is equal to 2, which confirms that this link is part of a mutual dependency, i.e., an interdependency. For this reason, node 22 has one interdependency that consists of one IoD_{Inter} and one SoD_{Inter}, and two dependency links, i.e., $2IoD_{Inter}$ because the WoD of these two links is equal to 2:

$$SoD_{Inter}(22) = 1, WoD(SoD_{Inter}(22)) = 2 \rightarrow (1\ Interdependency)$$
$$IoD_{Inter}(22) = 3, WoD(IoD_{Inter}(22)) = 4 \rightarrow (1\ Interdependency + 2\ Dependency)$$

The results obtained from the analysis of WoD, IoD_{Inter} and SoD_{Inter} are consistent with Figure 9. Therefore, the values of IoD_{Inter}, SoD_{Inter}, and the corresponding WoD of each node can be used to extract the properties of systems' connections. These features were not studied in previous works.

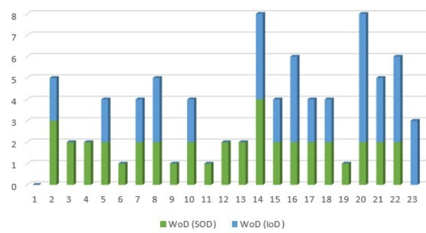


Figure 12. Weight of dependency for SoD and IoD of the test system.

In Section 3, we also argued that higher order of dependency (HoD) can provide a deeper understanding of interactions between the system components. To evaluate that, the third order of dependency for SoD_{Inter} and IoD_{Inter} of the test system is measured based on Equation (14), in which n = 3; the result is depicted in Figure 13. To date, based on the measured values shown in Figures 11 and 12, we showed that nodes $\{5, 7, 10, 14, 15, 17, 18\}$ are the end-users of the closed-loops that exist in the test system.

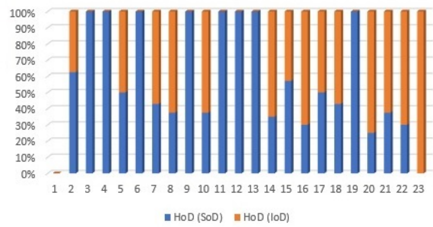


Figure 13. Higher order of dependency for SoD and IoD of the test system.

Notably, Figure 13 shows that even in the third order of dependency, the values of the SoD_{Inter} and IoD_{Inter} of nodes $\{5, 17\}$ are still equal. This means that nodes $\{5, 17\}$ form an isolated closed-loop in the system, in which both of these nodes are the end-users.

In addition, the nodes $\{3, 4, 6, 9, 11, 12, 13, 19, 23\}$ in Figure 11 have either the value of SoD or the value of IoD. Due to the fact that the values of the IoD_{Inter} of nodes $\{3, 4, 6, 9, 11, 12, 13, 19\}$ are equal to zero in Figure 13, these nodes are absolute receiver nodes in the interdependent part of the system. Likewise, given that the value of $SoD_{Inter}(23) = 0$ in Figure 13, node 23 is only a sender. If any of the absolute receiver nodes $\{3, 4, 6, 9, 11, 12, 13, 19\}$ in one subsystem fails, the other subsystem will not be affected (see Figure 9). To make it more clear, we remove each node of the test system and calculate the number of nodes that will be influenced by this removal. The result is depicted in Figure 14. In summary, Figure 14 highlights that removing the nodes with $HoD(IoD_{Inter}) = 0$ will cause no change in the interdependent part of the system while removing nodes with the higher value of $HoD(IoD_{Inter})$ has a major impact on the connectivity of other nodes.

Taking the higher order of dependency into consideration helps us to better understand the importance of links, and the role of nodes between two subsystems; this is of high value for risk management in complex systems.

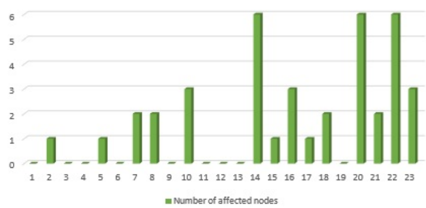


Figure 14. Number of affected nodes by removing each nodes of the test system.

The last parameter to investigate on the test system is the Criticality of Dependency (CoD). Based on the betweenness centrality and efficiency, Sanchez et al. [62] stated that nodes $\{1, 2, 20, 15, 19\}$ are vital nodes within this test system. In a follow-up paper [33], the authors expanded the study and introduced $\{2, 5, 8, 9, 16, 19, 20\}$ as critical nodes based on the Node Degree and weighted Efficiency. Aligned with these papers, a recent study conducted on this system ranked the criticality of each node based on the aggregation of three metrics that measure the importance of each node and its connected links in the entire system [63].

All these recent studies attempt to identify critical components in a complex system, while our purpose here is to determine the critical dependencies between two subsystems. The CoD in a system-of-systems assesses how close one node in a subsystem is to the critical nodes of the other subsystem; this allows us to identify potential vulnerable areas for further investigation. Indeed, once the CoD of a system-of-systems is measured, then we can concentrate on the analysis of other features such as the susceptibility or the impact of those dependencies that have a higher value of CoD in the system, and consequently take proper action to control the consequences, and reduce the risk based on that information.

To compute the Criticality of Dependency (CoD) of the test system, we utilize the ranking presented in [63], as it covers all the nodes of the system. Figure 15 displays the criticality of each node, the CoD, and the third order of dependency for the CoD.

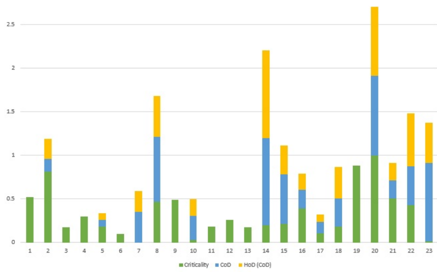


Figure 15. Criticality of nodes, CoD and higher order of dependency for CoD of the test system.

Regarding Figure 15, identified critical components in a system are not necessarily those components that have the main role in connecting two subsystems. It should be noticed that when two well-designed and secure systems are merged, the outcome is a system-of-systems in which even less important components of each subsystem might turn to critical components, because of the new linkages. For example, in Figure 15 although node 14 has been not identified as a highly critical node in the test system, its value of CoD indicates that node 14 has a close connection with critical nodes of the system. According to Figure 7, node 14, which is a bus in the first subsystem, is connected to node 20, the main ICT router and the most critical node in the second subsystem. Likewise, $\{8, 23\}$ are two other nodes with the noticeable value of CoD in Figure 15, which are connected to the critical nodes 19 and 8 (from the other subsystem), respectively. As depicted in Figure 9, apart from the interdependency between nodes 14 and 20, these nodes along with nodes $\{12, 13, 22\}$ form a local loop; this implies the existence of a vulnerable zone in the system-of-systems. In case that an event adversely affects the functionality of a node and a higher order of dependency turns back to that node, a feedback effect forms in the system which will influence other nodes as well and will exacerbate the total impact of the initial event. Analysis of the higher order of CoD in systems helps us to identify these vulnerable local loops.

The chain of dependency for node 14 shows a direct connection between node 14 (parent) and nodes $\{20, 22\}$ (children) as the first order of dependency, i.e., $14 \rightarrow [20, 22]$. The second order includes the connections of the children of node 14 which are $20 \rightarrow [3, 9, 12, 13, 14]$ and $22 \rightarrow [12, 13, 14]$. Among the children of the second order only node 14 has further linkages. Therefore, the third order contains the connection between node 14 (as a child in the second order of dependency) and $\{20, 22\}$. The chain of dependency for node 14 is as follows:

$14 \rightarrow 20 \rightarrow 3 \times |$
$14 \rightarrow 20 \rightarrow 9 \times |$
$14 \rightarrow 20 \rightarrow 12 \times |$
$14 \rightarrow 20 \rightarrow 13 \times |$
$14 \rightarrow 20 \rightarrow 14 \rightarrow 20|$
$14 \rightarrow 20 \rightarrow 14 \rightarrow 22|$
$14 \rightarrow 22 \rightarrow 12 \times |$

$14 \to 22 \to 13 \times |$
$14 \to 22 \to 14 \to 20|$
$14 \to 22 \to 14 \to 22|$

The desired length for extracting the chain of dependency could be adjusted depending on the scale of the system.

In addition to the test system discussed in this section, we developed several test systems with different, large numbers of nodes, in order to evaluate the scalability of the proposed method. All the tests were performed using Matlab R2020a with an Intel Core i7 2.11 GHz processor with 16 GB RAM. To ensure the accuracy of the result, each test was iterated 20 times and both average time and the maximum time recorded. Table 2 demonstrates the outcomes of this analysis. The run times reported in Table 2 show that MDSM can be effectively used to extract the characteristics of dependencies in large scale Cyber–Physical systems.

Table 2. Running time for computing dependency parameters considering the third order of dependency.

Number of Nodes	Avg. Time (per Second)	Max. Time (per Second)
50	0.0049308	0.016134
100	0.0224031	0.10466
500	0.10141165	0.187021
1000	0.40492025	0.440655
5000	29.62836675	30.875652

6. Application of Dependency Analysis

Developing a simple model to characterize the structural properties of CPSs such as the interdependencies between subsystems, is of paramount importance to understand and predict the behaviour of systems. What is more interesting is that such a model can be used to extract the chains of influence across multiple subsystems, thereby assisting the vulnerability analysis [64]. As mentioned earlier, MDSM is an intuitive method that can be used for modelling different types of system architectures to display the connections between subsystems within one complex system or the interactions between two critical infrastructures.

MDSM enables system designers and decision-makers to analyse the characteristics of connections inside CPSs to extract dependencies and interdependencies within these systems, to examine a variety of hypothetical scenarios and to anticipate different types of failures that might expand through these links across the entire system.

Dependency parameters of MDSM provide a valuable perspective on the impact of interdependency between subsystems and show how the failure of one subsystem has a domino effect on the others. MDSM provides deep insights into the behaviour of complex CPSs and contributes to system design and recovery as well as to the identification of potential failures and vulnerabilities, security enhancement strategies and risk mitigation. In short, extracting dependency relations in CPSs contributes to satisfying the following objectives:

- Identification of hidden vulnerable zones and dependencies among subsystems.
- Investigation of cascading failures based on the dependency chain inside the systems.
- Analysing the severity and impact of probable failures.
- System design modification in order to mitigate dependencies and consequent failures.
- Developing the system recovery and protection strategies.
- Enhancing the resilience of complex systems.
- Improvement of system security and safety.

7. Conclusions

In this paper, we proposed the Modified Dependency Structure Matrix (MDSM) to identify, demonstrate and analyse the characteristics of connections in large scale Cyber Physical Systems. MDSM is a graphical method which aims to provide a compact perspective of inter-dependencies and intra-dependencies that exist between subsystems of a complex system. The dependency parameters introduced in this method, namely Impact of Dependency (IoD), Susceptibility of Dependency (SoD), Weight of Dependency (WoD) and Criticality of Dependency (CoD) provide quantitative measures to determine the characteristics of dependencies among components and subsystems. Unlike previous works, by applying the concept of chain of dependency, MDSM can evaluate the role of each connection in the higher order dependencies and provide a comprehensive perspective regarding the importance of each connection. In general, dependency parameters help to design more reliable and secure complex systems by protecting the critical nodes of each subsystem from vulnerable nodes of the other subsystems and manage this distance by utilizing the chain of dependency at the desired level. The quantitative value of the dependency parameters provides a better view for system designers to modify the architecture of systems, and it helps decision-makers to enhance the security of the system by allocating the budget to more vulnerable zones. As discussed in Section 6, the possible applications of MDSM both as a graphical model and for acquiring dependency parameters are quite many. Among possible options, in future works, we will mainly focus on improving risk management methods as well as developing an attack path analysis model based on the interdependency analysis of CPSs.

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

Funding: This work was funded by the Research Council of Norway, Joint Indo-Norwegian Project "Cyber-Physical Security in Energy Infrastructure of Smart Cities" (CPSEC), Project No.: 280617.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97.
2. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control. Syst. Mag.* **2001**, *21*, 11–25.
3. Haes Alhelou, H.; Hamedani-Golshan, M.E.; Njenda, T.C.; Siano, P. A survey on power system blackout and cascading events: Research motivations and challenges. *Energies* **2019**, *12*, 682.
4. Shivakumar, A.; Welsch, M.; Taliotis, C.; Jakšić, D.; Baričević, T.; Howells, M.; Gupta, S.; Rogner, H. Valuing blackouts and lost leisure: Estimating electricity interruption costs for households across the European Union. *Energy Res. Soc. Sci.* **2017**, *34*, 39–48.
5. Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the cyber attack on the Ukrainian power grid: Defense Use Case. In proceedings of the Electricity Information Sharing and Analysis Center (E-ISAC), Washington DC USA, 18 March 2016.
6. Wu, Y.K.; Chang, S.M.; Hu, Y.L. Literature review of power system blackouts. *Energy Procedia* **2017**, *141*, 428–431.
7. Akbarzadeh, A.; Pandey, P.; Katsikas, S. Cyber-Physical Interdependencies in Power Plant Systems: A Review of Cyber Security Risks. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019; pp. 1–6.
8. Li, X.; Yu, W. A hybrid fuzzy petri nets and neural networks framework for modeling critical infrastructure systems. In Proceedings of the 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–6.
9. Beccuti, M.; Chiaradonna, S.; Di Giandomenico, F.; Donatelli, S.; Dondossola, G.; Franceschinis, G. Quantification of dependencies between electrical and information infrastructures. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 14–27.
10. Tan, R.R.; Aviso, K.B.; Promentilla, M.A.B.; Yu, K.D.S.; Santos, J.R. Input–Output Models of Infrastructure Systems. In *Input-Output Models for Sustainable Industrial Systems*; Springer: Singapore, 2019; pp. 63–74.
11. Hossain, N.U.I.; El Amrani, S.; Jaradat, R.; Marufuzzaman, M.; Buchanan, R.; Rinaudo, C.; Hamilton, M. Modeling and assessing interdependencies between critical infrastructures using Bayesian network: A case study of inland waterway port and surrounding supply chain network. *Reliab. Eng. Syst. Saf.* **2020**, *198*, 106898.

12. Wei, J.; Kundur, D. Biologically inspired hierarchical cyber-physical multi-agent distributed control framework for sustainable smart grids. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 219–259.
13. Laugé, A.; Hernantes, J.; Sarriegi, J.M. Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 16–23.
14. Iturriza, M.; Labaka, L.; Sarriegi, J.M.; Hernantes, J. Modelling methodologies for analysing critical infrastructures. *J. Simul.* **2018**, *12*, 128–143.
15. Carhart, N.; Rosenberg, G. A framework for characterising infrastructure interdependencies. *Int. J. Complex. Appl. Sci. Technol.* **2016**, *1*, 35–60.
16. Boccaletti, S.; Latora, V.; Moreno, Y.; Chavez, M.; Hwang, D.U. Complex networks: Structure and dynamics. *Phys. Rep.* **2006**, *424*, 175–308.
17. Blackwell, C. A multi-layered security architecture for modelling complex systems. In Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, Oak Ridge TN, USA, May 2008; pp. 1–4, doi:10.1145/1413140.1413180
18. Wallace, W.A.; Mendonça, D.; Lee, E.; Mitchell, J.; Chow, J. Managing disruptions to critical interdependent infrastructures in the context of the 2001 World Trade Center attack. In *Jacquelyn L. Monday (Ed.); Beyond September 11th: An Account of Post-Disaster Research*; Institute of Behavioral Science, Natural Hazards Research and Applications Information Center, University of Colorado: Boulder, CO, USA, 2003.
19. Zhang, P.; Peeta, S. A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transp. Res. Part B Methodol.* **2011**, *45*, 553–579.
20. Dudenhoeffer, D.D.; Permann, M.R.; Manic, M. CIMS: A framework for infrastructure interdependency modeling and analysis. In Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, USA, 3–6 December 2006; pp. 478–485.
21. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 43–60.
22. Nieuwenhuijs, A.; Luiijf, E.; Klaver, M. Modeling dependencies in critical infrastructures. In Proceedings of the International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 12–14 March 2008; pp. 205–213.
23. Van Eeten, M.; Nieuwenhuijs, A.; Luiijf, E.; Klaver, M.; Cruz, E. The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Adm.* **2011**, *89*, 381–400.
24. Rausand, M.; Haugen, S. *Risk Assessment: Theory, Methods, and Applications, 2nd Edition*; John Wiley & Sons: Hoboken, NJ, USA, 2020.
25. Falahati, B.; Fu, Y. Reliability assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Trans. Smart Grid* **2014**, *5*, 1677–1685.
26. Kotzanikolaou, P.; Theoharidou, M.; Gritzalis, D. Assessing n-order dependencies between critical infrastructures. *Int. J. Crit. Infrastructures* **2013**, *9*, 93–110.
27. Mathew, J.; Ma, L.; Tan, A.; Weijnen, M.; Lee, J. Engineering asset management and infrastructure sustainability. In Proceedings of the 5th World Congress on Engineering Asset Management (WCEAM 2010), Cincinnati, OH, USA, 3–5 October 2011.
28. Luiijf, E.; Nieuwenhuijs, A.; Klaver, M.; van Eeten, M.; Cruz, E. Empirical findings on critical infrastructure dependencies in Europe. In Proceedings of the International Workshop on Critical Information Infrastructures Security, Rome, Italy, 13–15 October 2008; pp. 302–310.
29. Macaulay, T. *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*; CRC Press: Boca Raton, FL, USA, 2008.
30. Turoff, M.; Bañuls, V.A.; Plotnick, L.; Hiltz, S.R.; de la Huerga, M.R. A collaborative dynamic scenario model for the interaction of critical infrastructures. *Futures* **2016**, *84*, 23–42.
31. Faramehr, S. Investigating Dependencies between Railway System and Other Infrastructure Systems: Using a Scenario-Based Case Study Approach. Ph.D. Thesis, UCL (Univeristy College London), London, UK, 2020.
32. Zhang, Y.; Yang, N.; Lall, U. Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. *J. Syst. Sci. Syst. Eng.* **2016**, *25*, 102–118.
33. Milanović, J.V.; Zhu, W. Modeling of interconnected critical infrastructure systems using complex network theory. *IEEE Trans. Smart Grid* **2017**, *9*, 4637–4648.
34. Wang, Y.; Yan, G. A new model approach of electrical cyber physical systems considering cyber security. *IEEJ Trans. Electr. Electron. Eng.* **2019**, *14*, 201–213.
35. Tøndel, I.A.; Foros, J.; Kilskar, S.S.; Hokstad, P.; Jaatun, M.G. Interdependencies and reliability in the combined ICT and power system: An overview of current research. *Appl. Comput. Inform.* **2018**, *14*, 17–27.
36. Wirtz, N.; Monti, A. A Flexible Framework to Investigate Cascading in Interdependent Networks of Power Systems. In Proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon), 1 October–28 September 2020; pp. 38–41.
37. Sen, A.; Basu, K. On connectivity of interdependent networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
38. Satumtira, G.; Dueñas-Osorio, L. Synthesis of modeling and simulation methods on critical infrastructure interdependencies research. In *Sustainable and Resilient Critical Infrastructure Systems*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–51.

39. Haimes, Y.Y.; Jiang, P. Leontief-based model of risk in complex interconnected infrastructures. *J. Infrastruct. Syst.* **2001**, *7*, 1–12.
40. Setola, R.; Theocharidou, M. Modelling dependencies between critical infrastructures. In *Managing the Complexity of Critical Infrastructures*; Springer: Cham, Switzerland, 2016; pp. 19–41.
41. Johansson, J.; Hassel, H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 1335–1344.
42. Torres, J.L.S. Vulnerability, Interdependencies and Risk Analysis of Coupled Infrastructures: Power Distribution Network and ICT. Ph.D. Thesis, Université de Grenoble, Grenoble, France, 2013.
43. Hadjsaid, N.; Tranchita, C.; Rozel, B.; Viziteu, M.; Caire, R. Modeling cyber and physical interdependencies-Application in ICT and power grids. In Proceedings of the 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–6.
44. Rosato, V.; Issacharoff, L.; Tiriticco, F.; Meloni, S.; Porcellinis, S.; Setola, R. Modelling interdependent infrastructures using interacting dynamical models. *Int. J. Crit. Infrastructures* **2008**, *4*, 63–79.
45. Fioriti, V.; D'Agostino, G.; Bologna, S. On modeling and measuring inter-dependencies among critical infrastructures. In Proceedings of the 2010 Complexity in Engineering, Rome, Italy, 22–24 February 2010; pp. 85–87.
46. Gueye, A.; Mbaye, B.; Fall, D.; Diop, A.; Kashihara, S. A Matrix Model to Analyze Cascading Failure in Critical Infrastructures. In Proceedings of the International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas, Nairobi, Kenya, 8–9 March 2020; pp. 211–223.
47. Chen, L.; Whyte, J. Analysing interdependencies of complex engineering systems using a digital twin-driven design structure matrix. In Proceedings of the Construction Research Congress 2020: Computer Applications. American Society of Civil Engineers Reston, Reston, VA, USA, 5–7 April 2020; pp. 417–426.
48. Peterson, T. Exploring System Space with Graph Theory. In Proceedings of the INCOSE International Symposium, Scotland, UK, 18–21 July 2016; Volume 26, pp. 1120–1128.
49. Austin, S.; Baldwin, A.; Li, B.; Waskett, P. Analytical design planning technique (ADePT): a dependency structure matrix tool to schedule the building design process. *Constr. Manag. Econ.* **2000**, *18*, 173–182.
50. Eppinger, S.D.; Browning, T.R. *Design Structure Matrix Methods and Applications*; MIT Press: Cambridge, MA, USA, 2012.
51. Thulasiraman, K.; Arumugam, S.; Nishizeki, T.; Brandstädt, A.; et al. *Handbook of Graph Theory, Combinatorial Optimization, and Algorithms*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2016.
52. Barabási, A.L.; Bonabeau, E. Scale-free networks. *Sci. Am.* **2003**, *288*, 60–69.
53. Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Controllability of complex networks. *Nature* **2011**, *473*, 167–173.
54. Gen, M.; Cheng, R.; Lin, L. *Network Models and Optimization: Multiobjective Genetic Algorithm Approach*; Springer: London, UK, 2008.
55. Selim, S.Z.; Alsultan, K. A simulated annealing algorithm for the clustering problem. *Pattern Recognit.* **1991**, *24*, 1003–1008.
56. Dorigo, M.; Gambardella, L.M. Ant colony system: A cooperative learning approach to the traveling salesman problem. *IEEE Trans. Evol. Comput.* **1997**, *1*, 53–66.
57. Atashpaz-Gargari, E.; Lucas, C. Imperialist competitive algorithm: an algorithm for optimization inspired by imperialistic competition. In Proceedings of the 2007 IEEE Congress on Evolutionary Computation, Singapore, 25–28 September 2007; pp. 4661–4667.
58. Hosseini, S.; Al Khaled, A. A survey on the imperialist competitive algorithm metaheuristic: implementation in engineering domain and directions for future research. *Appl. Soft Comput.* **2014**, *24*, 1078–1094.
59. Guariniello, C.; DeLaurentis, D. Supporting design via the system operational dependency analysis methodology. *Res. Eng. Des.* **2017**, *28*, 53–69.
60. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028.
61. Bang-Jensen, J.; Gutin, G.Z. *Digraphs: Theory, Algorithms and Applications*; Springer: London, UK, 2008.
62. Sanchez, J.; Caire, R.; Hadjsaid, N. Ict and electric power systems interdependencies modeling. In Proceedings of the International ETG-Congress 2013, Symposium 1: Security in Critical Infrastructures Today, Berlin, Germany, 5–6 November 2013; pp. 1–6.
63. Akbarzadeh, A.; Katsikas, S. Identifying Critical Components in Large Scale Cyber Physical Systems. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, Seoul, Korea, 27 June–19 July 2020; pp. 230–236.
64. Stapelberg, R.F. Infrastructure systems interdependencies and risk informed decision making (RIDM): impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards. *J. Syst. Cybern. Inform.* **2008**, *6*, 21–27.

10 Article IV: Dependency-based Risk Assessment for Cyber-Physical systems [5]

International Journal of Information Security
https://doi.org/10.1007/s10207-022-00608-4

SPECIAL ISSUE PAPER

Dependency-based security risk assessment for cyber-physical systems

Aida Akbarzadeh[1] · Sokratis K. Katsikas[1]

Abstract

A cyber-physical attack is a security breach in cyber space that impacts on the physical environment. The number and diversity of such attacks against Cyber-Physical Systems (CPSs) are increasing at impressive rates. In times of Industry 4.0 and Cyber-Physical Systems, providing security against cyber-physical attacks is a serious challenge which calls for cybersecurity risk assessment methods capable of investigating the tight interactions and interdependencies between the cyber and the physical components in such systems. However, existing risk assessment methods do not consider this specific characteristic of CPSs. In this paper, we propose a dependency-based, domain-agnostic cybersecurity risk assessment method that leverages a model of the CPS under study that captures dependencies among the system components. The proposed method identifies possible attack paths against critical components of a CPS by taking an attacker's viewpoint and prioritizes these paths according to their risk to materialize, thus allowing the defenders to define efficient security controls. We illustrate the workings of the proposed method by applying it to a case study of a CPS in the energy domain, and we highlight the advantages that the proposed method offers when used to assess cybersecurity risks in CPSs.

Keywords Cyber-physical systems · Attack path analysis · Risk assessment · Safety · Security · Industrial control systems · Industry 4.0

1 Introduction

The merging of Information and Communication Technology (ICT) with Operational Technology (OT) has formed Cyber Physical Systems. The advantages of this merging in the monitoring and control of traditional industrial control systems notwithstanding [1], the interdependencies between the cyber and the physical parts of CPSs cause new types of cybersecurity risks, as cyber components may adversely affect the physical environment, thereby increasing safety risks. For instance, in the Maroochy attack, by leveraging the cyber parts of the Maroochy county water service, an attacker gained remote access to the control system which enabled him to affect pumping stations [2]. He gradually discharged 800,000 L of raw sewage into the river; this had a severe impact on nature reserves, on wildlife, as well as on the local population. Stuxnet [3] and attack to Florida water treatment plant [4] are two other examples of cyber-physical attacks.

In a CPS, unexpected events mainly stem from the overly convoluted connections and interdependencies among its heterogeneous components. Castellanos et al. [5] shed light on the new risks that direct and undirect dependencies between cyber and physical components bring to Industrial Control Systems (ICSs) that form the core of cyber-physical systems. These dependencies further accentuate when the CPS is a system-of-systems. Alcaraz et al. [6] also reviewed the emerging challenges of protecting industrial control systems and pointed out the fact that the different mindsets between IT and OT operators regarding the security risk in CPSs is one of the main reasons that these dependencies are still neglected.

The diversity of assets and of the interactions among them in a CPS is an additional reason why traditional risk assessment methods are not able to identify cyber physical attacks, as the scope of analysis in these methods is limited to pure IT systems. Recent works have proposed merging previously developed security and safety risk assessment methods. However, these integrated methods do not address the cyber-physical and physical-cyber interdependencies in

Aida Akbarzadeh
aida.akbarzadeh@ntnu.no

Sokratis K. Katsikas
sokratis.katsikas@ntnu.no

1 Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Published online: 22 August 2022

the assessment, as the constituents have been developed separately, with focus on either the physical or the cyber facets of CPSs. Indeed, traditional CPSs were built as physically and logically isolated systems, air-gaped systems, with no security mechanisms in place except for physical security measures. Later, these systems were gradually augmented with networking functionality and could connect to the Internet and provide remote monitoring and control [7].

Cyber-physical systems are known as complex systems, and this characteristic mainly stems from the multiple types of connections, different system topologies and various structures of subsystems in a cyber-physical system. Moving toward Industry 4.0 will significantly increase this complexity. Consequently, systems comprising identical assets may face different security risks. As a result, risk assessment should focus on the interactions and relations between the assets of a CPS rather than merely on the assets themselves. This requires a precise investigation from the physical field devices up to the cyber management systems to cover every aspect of the system; in other words, an "end-to-end" investigation is required to cover both IT and OT with a unified approach.

The IEC TS 62351-1:2007 standard [8] states that providing 100% security for each system component not only counts as a costly and impractical solution, but also might discourage enterprises attempting to utilize security mechanisms. Therefore, risk assessment methods for CPSs need to pay special attention to increasing the efficiency and avoiding unnecessary analysis that is of no value to enhancing the security of the system. Wang et al. [9] also stated that attacks to CPSs have unique characteristics, as adversaries have a clear attack target and aim to damage the operational part of the systems to different extent. As a result, improving the security of CPSs highly depends on extracting the sequence of attack steps toward the adversaries' target. This implies that risk assessment methods in CPSs should follow a goal-oriented approach, to enhance effectiveness and improve accuracy.

One approach to conduct an end-to-end risk assessment is to leverage attack path analysis [10]. An attack path specifies an attack scenario and a sequence of assets that can be used by attackers to reach to their goal. Indeed, each attack composed of different phases that must be proceed step-by-step to reach its final objective, known as "kill chain" [11]. In other words, each attack could be seen as a chain of dependency. Therefore, to prevent the attacker from reaching its goal and influence the system, it is enough to break the linkages of this chain. Only one disruption in the attack path can protect the system. Accordingly, a new notion for an "end-to-end" protection can be defined, in which the "end-to-end" safety and security implies the absence of a dependency chain between the two corresponding components. In this case, security and safety flaws of individual assets are accepted as long as adversaries cannot leverage them to make a semantic path within the system. However, attack path analysis is an IT-related method whose main focus is to understand how attackers gain access to their victim asset and which vulnerabilities can be exploited on which assets. Cyber-physical systems are different in nature; this should be considered when developing a method based on attack path analysis. Besides, the emerging cyber-physical attacks have shown that in many cases adversaries attempt to interrupt the physical process of the system or to damage physical components that are supposed to be isolated by air gaps [12–14]. Unlike IT systems, affecting the functionality of industrial control systems is most often the target of complex cyber attacks in CPSs. Therefore, a unified IT&OT risk assessment, i.e., a general risk assessment of a CPS, requires the contribution of OT experts to clear the goal of potential attacks toward field devices on one hand, and of IT experts to provide a complete picture of how an attacker might be able to reach their target component and affect the system on the other.

Acknowledging the advantages of leveraging attack path analysis to draw a clear picture of possible attacks against a CPS and considering the specific attributes of CPSs, in this paper we propose a novel, dependency-based risk assessment method. The method first identifies the critical assets of the system and then, discovers chains of dependencies between pertinent assets that might be leveraged by attackers to reach their target. The proposed method is a comprehensive method that considers both the topological and functional relationships between the system components as direct and hidden dependencies within the CPS, to provide a holistic risk assessment. It utilizes Bow Tie modeling for visualizing security risks to facilitate the collaboration between IT and OT experts in CPSs and assists the defenders in understanding the intention of attackers, thus guiding them to employ relevant approaches to mitigate the accordant risks. It also helps defenders to discover those potential attack paths that may be created in case of a zero-day vulnerability. The proposed method is domain-agnostic and has been developed to cover all CPSs in different domains, such as Maritime, Aviation and Energy. In this work, we showcase the workings of the proposed method in a case study of a CPS in the energy domain, as an example.

The main contribution of this paper is as follows: We propose a dependency-based risk assessment method to extract goal-oriented attack paths in CPSs that considers cyber-physical and physical-cyber interdependencies within the systems. The proposed method:

– Facilitates the collaboration between IT and OT experts to identify unwanted events from both safety and security perspectives based on the Bow Tie model.

– Reveals complex cyber-physical attacks by employing backtrack analysis to understand the intention of attackers.
– Improves the effectiveness of attack path analysis by replacing blind analysis with goal-oriented backtrack analysis.
– Is a realistic method to compute risk and to assess Likelihood and Impact based on metrics that cover both IT and OT requirements.

The remainder of the paper is organized as follows: Sect. 2 reviews the related work. We describe the proposed method in Sect. 3, and a case study to expound the application of the proposed method is presented in Sect. 4. We discuss our findings in Sects. 5 and 6 summarizes our conclusions and indicates directions for future work.

2 Related work

A wealth of security risk assessment methods applicable to general purpose IT systems exists [15]. Even though several of these methods can be and have been applied to Cyber Physical Systems, they cannot accurately assess cyber risks related to CPSs [16]. Among different methods, threat modeling approaches such as STRIDE [17], Factor Analysis of Information Risk (FAIR) [18] and OCTAVE [19] have been applied to assess risk in CPSs operating in various domains. Combining two or more methods, mainly STRIDE and CVSS, is also a common approach to achieve better performance [20].

Alcaraz et al. [6] reviewed the emerging challenges of protecting industrial control systems and pointed to the urgent necessity of developing new mechanisms and recommendations. The authors argued that the integration of old technologies such as SCADA systems with modern communication networks and the different mindsets of IT and OT operators regarding the security risk is the core underlying factor that escalates these challenges and affects the security of the systems. In a follow-up paper, the authors studied different aspects of control systems in CPSs and concluded that OT assets such as RTUs and Data historians are of the most targeted and vulnerable assets in a CPS due to the fact that targeting these components not only imposes risks to sensitive information but also to the operational activities and processes in the system and all the dependent subsystems.

Cyber risk assessment methods for CPSs more often than not are domain specific, as they need to take into account safety as an impact factor additional to the “traditional” impact factors of confidentiality, integrity, and availability. This is why security and safety of CPSs are studied jointly. A comprehensive survey of security and safety co-engineering methods is provided in [21]. An overview of risk assessment methods specific to the smart grid case is provided in [22]. Kandasamy et al. [23] presented an overview of risk assessment methods for the Internet of Things. A review of risk assessment methods for SCADA systems is presented in [24]. Threat and risk assessment techniques for the automotive domain are reviewed in [25].

A number of approaches for risk assessment for CPSs, published before 2015, are listed in [16]. The list is not exhaustive, nor do the authors indicate how the listed works were selected. A more recent review of a few risk assessment methods for CPS, from the perspective of safety, security, and their integration, including a proposal for some classification criteria was made in [26].

Recently, Stellios et al. [7] proposed a high-level risk assessment approach for IoT-enabled cyber-physical systems with the emphasis on the identification of attack paths and explained the necessity for considering connectivity attack paths and functionality attack paths in CPSs. However, their work is limited to guidance, without any technical detail or case study.

Existing risk assessment methods for CPSs consider only the cyber or the physical part of the system, while cyber-physical and physical-cyber interdependencies are by and large left unattended. For example, Homer et al. [27] only considered the cyber parts of the system, while the authors in [28] focused on the physical parts. This is despite that, as Krotofil et al. [29] showed, attackers can leverage the physics of the process underlying a CPS to conduct their attack. The same authors suggested that when defining security measures, the physical process layer should be considered as well. As mentioned in [30], a holistic approach to studying the cyber physical systems is required which can handle the complex coupling between the physical process and the IT infrastructure.

However, to the best of our knowledge, a risk assessment method that satisfies this requirement has not been proposed. The method proposed in this paper addresses this research gap. Indeed, unlike existing methods, the method proposed herein facilitates the analysis of the entire cyber-physical system, for each unwanted event. Thus, it provides a clear picture of involved parts of the system and reveals the hidden dependencies and the potential infiltration points across the system.

3 Risk assessment methodology

This section describes the structure of the proposed risk assessment methodology. As shown in Fig. 1, the proposed method is divided into four phases. To conduct a holistic risk assessment for cyber-physical systems, we first need to model the system, to find connections and dependencies between the system components; this is done in Phase I. This will facilitate the identification of dependency chains and the use of the bow-tie methodology which will be described later, in Phase III. Once we have modeled the system, we identify and rank the criticality of the system components, as the proposed method begins the risk analysis with the vital components; this is done in Phase II. Considering the numerous components that constitute a CPS, in particular a large-scale cyber-physical system, this approach enhances efficiency and enables system owners with limited information and resources to apply the proposed risk assessment method only to critical components in their system; however, a complete analysis is always recommended. In Phase III, for each target component selected according to the result of Phase II, we perform a depth-first search to extract dependency chains. Then, we identify all unwanted events for the target components and investigate whether each extracted dependency chain can actually lead to that unwanted event. It is worth mentioning that the main goal of this phase is to enable both IT and OT operators to investigate the preconditions that can lead to a specified unwanted event, from both a safety and a security perspective. Additionally, as the unwanted events can affect both the safety and the security of a system, it is required to consider the risk from both perspectives. Risk is generally computed based on the Likelihood of an event occurring and the resulting Impact of the event. Therefore, to calculate risk, we collect pertinent metrics to measure Likelihood and Impact form both a safety and a security perspective. This will be described in further detail in Phase III. Finally, after computing the risk of each identified dependency chain, we rank the results. In the following, we describe each phase in more detail.

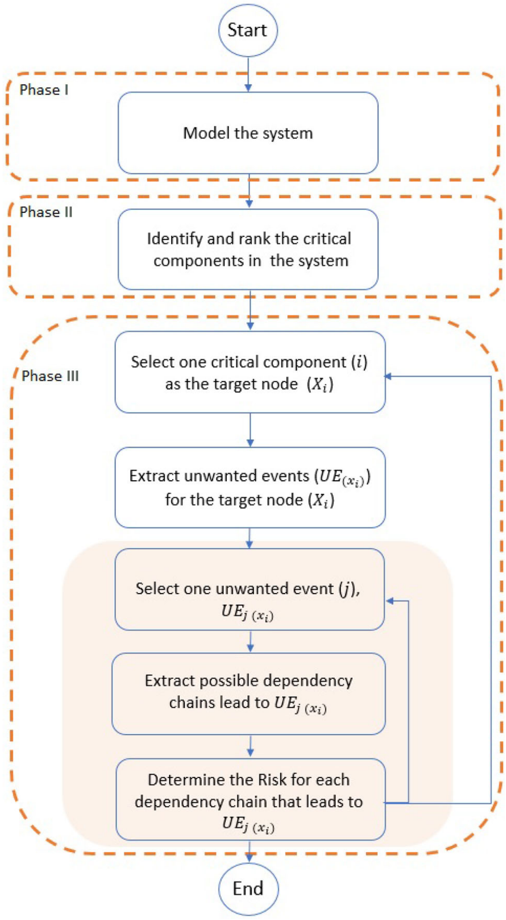


Fig. 1 Proposed risk assessment method

3.1 Phase I: Model the system

Presenting a comprehensive model of a CPS appropriate for assessing cybersecurity risks requires capturing both the topological and functional aspects of the system. Therefore, the first step is to capture the connections within the system and identify the cyber and physical interactions in the system which denote the data flows and the material flows in the system, respectively. A method that has been widely applied in recent works to model a CPS is graph theory [31,32]. Using graph theory, a CPS is modeled as a directed graph $G(V, E)$ in which V is a set of vertices (nodes) representing the components of the system and E is a set of edges (links) representing interconnections between the system components.

3.2 Phase II: Identify and rank the critical components in the system

The goal of this step is to rank the criticality of the system components as potential targets for cyber physical attacks, from both the system and the organizational perspective. This provides a macroscopic view of the system components and measures how important each component is, in case of accidental failures or deliberate attacks.

At the system level, the method presented in [33] is applied to measure the criticality. According to this method, the contribution of the system components, both the links and nodes, in preserving the system functionality and connectivity is evaluated. In more detail, the method of [33] utilizes the Closeness Centrality (CC) and two other novel graph metrics, namely the Tacit Input Centrality (TIC) and the Tacit Output Centrality (TOC), to measure the importance of nodes and links in a CPS. Then, by means of a multiple attribute decision making (MADM) approach, it aggregates these three metrics into the so-called Z-index and ranks the components of the CPS according to their criticality.

At the organizational level, the assistance of the system owners is required, as various factors such as economic effect and environmental effect are involved in the determination of the criticality. Indeed, at the system level, the main focus is solely on the characteristics and roles of the components, while at the organizational level, different aspects should be considered, e.g., the cost of repair and maintenance of the system components. Stakeholders assign one of the following values to determine the importance of each component at the organizational level:

– 1: Low importance;
– 2: Medium importance;
– 3: High importance.

Since the organizational level criticality is measured qualitatively, it should be scaled properly before aggregating with the result of the system level criticality. The overall criticality of a component X_i is calculated based on Eq. 1, in which C_{Org} and C_{Sys} refer to the organizational level criticality and the system level criticality, respectively.

$$C_{\text{Total}}(X_i) = \frac{C_{\text{Org}}(X_i)}{\max(C_{\text{Org}})} \times \max(C_{\text{Sys}}) + C_{\text{Sys}}(X_i) \quad (1)$$

3.3 Phase III: Dependency-based risk assessment

3.3.1 Extract dependency chains

Adversaries tend to target critical components in a system. Therefore, this step aims to identify possible chains of dependencies between the system components that might be leveraged by attackers to reach their desire goal. In an ideal situation, the risk assessment proposed in this paper begins with the most vital components ranked in phase II and continues to the level of criticality that the system owners are satisfied with. Clearly, it is possible to apply the method to all components. As illustrated in Fig. 1, phase III begins with selecting one of the critical components of the system as the target node X_i. Next, all unwanted events $\text{UE}_{(X_i)}$ that might affect node X_i are identified. It should be noted that the term *unwanted event* means *top event* in safety risk assessment and *incident* in cybersecurity risk assessment [34].

Then, one of the unwanted events that can influence node X_i is selected for further study (i.e., $\text{UE}_{j(X_i)}$). By performing a depth-first search, all the non-circular dependency chains that terminate at X_i are discovered.

In order to conduct the cybersecurity risk analysis along with the dependency chain, we apply the concept of bow-tie methodology. Since bow-tie modeling provides a visual representation of the hazards/threats and corresponding unwanted events, it can facilitate risk analysis in CPSs and bridge the gap between experts with different backgrounds

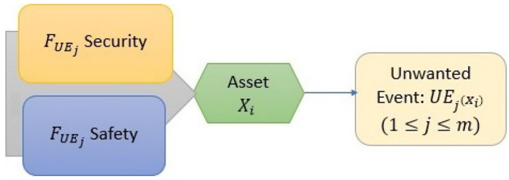


Fig. 2 Bow-tie

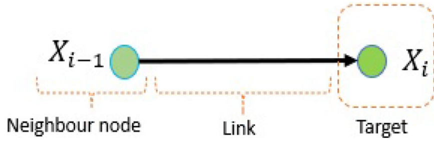


Fig. 3 Investigation of relationships in a dependency chain

and knowledge (e.g., IT and OT). The bow-tie analysis has been broadly used in safety risk management to identify root causes and consequences of hazards. Bernsmed et al. [34] applied bow-tie modeling to study the cybersecurity risks of maritime navigational systems and provided a common terminology for both safety and security risks which is adapted in our method. As depicted in Fig. 2, the right side of the bow-tie in our work corresponds to unwanted events ($\text{UE}_{j(x_i)}$) that might occur, the left side specifies the causes (F_{UE_j}) that can lead to these unwanted events, and the central knot marks the asset under study (X_i).

Assume that for the critical node X_i, $\text{UE}_{(X_i)} = \{\text{UE}_{1(X_i)}, \ldots, \text{UE}_{m(X_i)}\}$ are m possible unwanted events. To discover the attack paths that target node X_i, we start from node X_i and select the first unwanted event ($\text{UE}_{1(X_i)}$). Then, we check potential hazards and threats that can lead up to that event by considering node X_i, node X_{i-1} and link (X_{i-1}, X_i) as the corresponding attack surface of X_i (see Fig. 3).

If the cause of $\text{UE}_{1(X_i)}$ is found (called F_{UE_1}), we move one step to the left of the chain and repeat the same process for the next node (i.e., X_{i-1}). F_{UE_1} is any vulnerability or failure mode that can cause $\text{UE}_{1(X_i)}$. This process will terminate when there is no cause and effect relation between the neighbor nodes in a chain; the last node under the study denotes the *infiltration point* into the system (Fig. 4).

Considering asset X_i, F_{UE_j} points to the pre-condition j which, if met, will allow the post-condition (i.e., the unwanted event) $\text{UE}_{j_{(x_i)}}$ to occur. From the safety perspective, the pre-condition determines the failure modes and considers damage to property including X_i, X_{i-1} and link (X_{i-1}, X_i), while the post-condition shows the final effects and consequences of materializing each pre-condition. From the security perspective, affecting the confidentiality, integrity and availability is part of the pre-

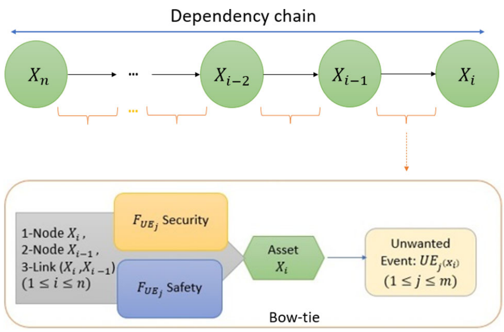


Fig. 4 Dependency chain and joint safety security risk analysis

condition, and the post-condition represents the goal of an attacker when targeting X_i, X_{i-1} or link (X_{i-1}, X_i).

It is worth emphasizing that, unlike previous works, we applied a backtracking approach to increase efficiency. Due to the fact that the goal of the risk assessment is clear from the beginning, here the attack paths and afterward the risk to each target component X_i can be computed separately with no need to investigate all the interactions and dependencies within a system. This approach also enables operators to view the system from the attackers' perspective and detect new attack paths that might exploit vulnerabilities that have been neglected during the system design.

To make it clear, consider the simple graph of Fig. 5. In this example, suppose that we are interested to detect attack paths that terminate at X_1 and cause $\mathrm{UE}1_{(x_1)}$. Here, we assume that vulnerabilities and failure modes exist between $X_7 \to X_3 \to X_1$ and $X_{12} \to X_9 \to X_5 \to X_1$ that can be leveraged by attackers and consequently lead to $\mathrm{UE}1_{(x_1)}$. Following the proposed method, we start the investigation from X_1 and move backwards to neighbor nodes $\{X_3, X_4, X_5\}$. Referring to the assumption, since there is no pre-condition F_{UE_j} that can lead to $\mathrm{UE}1_{(x_1)}$ from X_5, investigation from node X_5 will be terminated and this node will be removed from the list. The investigation continues until Path 1 and Path 2 are found. Notice that in Path 2, although there is a link between X_{12} and X_{13}, the process of detecting attack path terminates at X_{12} for the same reason explained earlier. Now, imagine that one attempts to discover the same attack paths by performing the straightforward approach. In this case, s/he should discover all paths terminating at X_1 and starting at the rest of nodes (i.e., $\{X_2, X_3, \ldots, X14\}$) to make sure that all the attack paths have been extracted. Therefore, not all identified attack paths will be related to the target component X_1 and the unwanted event $UE1_{(x_1)}$, as follows:

$$X_{14} \to X_{13} \to X_{10} \to X_6 \to X_2$$

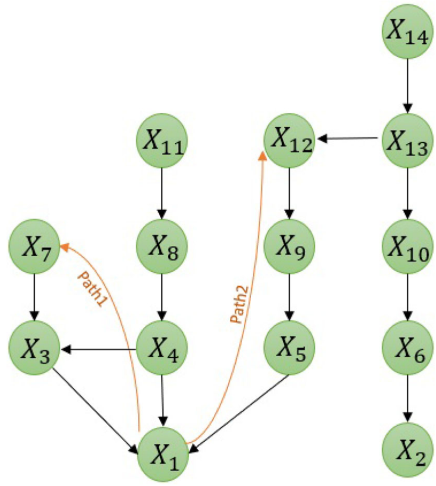


Fig. 5 A simple example of detecting attack paths

$$X_{14} \to X_{13} \to X_{12} \to X_9 \to X_5 \to X_1$$
$$X_{11} \to X_8 \to X_4 \to X_3 \to X_1$$
$$X_{11} \to X_8 \to X_4 \to X_1$$
$$X_7 \to X_3 \to X_1$$

Notice that, although there are dependencies between the components as depicted in Fig. 5, not all of them lead to $\mathrm{UE}1_{(x_1)}$. Therefore, by determining the unwanted event and moving backwards, our method prevents blind investigation and can enhance the scalability and efficiency compared to the previous ones.

3.3.2 Compute the risk

The last step of phase III is to compute the risk. The dependency chain illustrated in Fig. 4 clarifies that a critical component in a system will not be affected unless all the pre-conditions of its pertinent dependency chains are fulfilled. Accordingly, to compute the risk of each attack path that may lead to $\mathrm{UE}_{j(X_i)}$, the likelihood of that path being possible to materialize should be calculated. Generally, the probability of an unwanted event occurring (i.e., the Likelihood) multiplied by the magnitude of the consequences (i.e., the Impact) of that event gives an estimate of the risk. Thus, for critical node X_0, risk of materializing an attack path $X_n \to \cdots \to X_1 \to X_0$ with length n is calculated as follows [35]:

$$R_{\mathrm{Path}} = L_{X_n,\ldots,X_0} \times I_{X_1,X_0} = \prod_{i=0}^{n-1} L_{X_i,X_{i+1}} \times I_{X_1,X_0} \quad (2)$$

where R_{Path} denotes the risk of this attack path. L_i and I_i are the likelihood and impact of targeting X_0, respectively. However, there might be several attack paths toward a critical node X_i and the more paths a target node receives, the higher level of susceptibility and risk it has, as adversaries have several alternatives to target it [36]. To reflect this in computing the risk of each target node X_i, we adopt the concept of risk in [34] and we utilize Eq. 3 below. Here, $P(X_i)$ is the probability of accessing node X_i, which portrays the number of attack paths, and $\text{Impact}(X_i)$ denotes the impact resulting when $\text{UE}_{j(X_i)}$ occurs.

$$R(X_i) = P(X_i) \times \text{Impact}(X_i) \tag{3}$$

Due to the fact that identified attack paths for each target node X_i are mutually independent [34], the probability of accessing X_i through at least one of the available attack paths is computed based on Eq. 4.

$$P(X) = 1 - \prod_{i=1}^{k}(1 - p(\text{path}_i)) = 1 - \prod_{i=1}^{k}(1 - L_{X_n,\ldots,X_0}) \tag{4}$$

where $p(\text{path}_i)$ is the likelihood of the attack path i. As Bernsmed et al. [34] asserted, applying this approach to compute the probability of successful attack leads to more realistic results.

It then remains to determine the likelihood and impact. As mentioned earlier, the main objective of the proposed method is to facilitate concurrent analysis of safety and security risks in a CPS. This requires to compute likelihood and impact of an unwanted event based on metrics that contribute to both safety and security. For instance, from the security perspective, an unwanted event might have impact on confidentiality, integrity or availability of a system component and this impact mainly is limited to the system. However, from the safety perspective, this impact includes the environment in which the system is operating and other metrics such as economic effect, public effect and environmental effect should be considered. Therefore, to perform a comprehensive risk assessment for a CPS which encompasses both IT and OT components, we need to assess the impact based on both perspectives. To this end, we leveraged expert knowledge and related methods, mainly stemming from the CVSS Base Metrics [37], and summarized factors affecting the measurement of impact and likelihood in cyber-physical systems as shown in Tables 1 and 2.

Considering both cyber and physical aspects of a CPS, three metrics, namely *Access Vector (AV)*, *Required Knowledge/Skill (KS)* and *External Factors (EF)* are assessed to determine the likelihood. The *Access Vector* metric captures how an attacker can get access to the target component and how difficult this will be. For example, the likelihood of a successful attack when a component can be targeted remotely from outside of the system via the Internet is clearly higher than in the case when the component only can be manipulated via physical access, such as by inserting a USB. The *Required Knowledge/Skill* metric captures the complexity of the attack. This is a significant factor particularly when targeting the OT part in a CPS, as it requires domain knowledge that makes it relatively harder than targeting the IT part. Further, sometimes, in order for an attack to be successful, it must be conducted at a specific time or situation. For instance, in a power plant, improper synchronization can damage a generator only if it happens during a specific time window before the protection device actuates [38]; this will be discussed in some more detail in Sect. 4. A false data injection attack can be seen as another example, in which adversaries need to send false data in a specific time interval to be able to put the system in an unstable situation. Such factors are captured by the *External Factors (EF)* metric. Tables 1 and 2 provide detailed guidance in assigning values to the elements of risk.

The authors in [39] explained that the Likelihood and the Impact score are equal to the average of their constituent metrics. Therefore, by following the approach represented in [39], we compute the Likelihood and the Impact of exploiting a vulnerability or hazard in a dependency chain based on the average of the corresponding metrics defined in Tables 1 and 2 as follows:

$$\text{Likelihood} = \frac{\text{AV} + \text{KS} + \text{EF}}{3} \tag{5}$$

$$\text{Impact} = \frac{\text{Ec} + \text{P} + \text{En} + \text{C} + \text{A} + \text{I}}{6} \tag{6}$$

The scores range from 0 to 1.

It should be noted that, although cyber physical systems are most often composed of numerous components, these components can be classified into a few distinct groups. Based on the data provided by the MITRE Corporation,[1] devices in ICSs from different domains can be classified into seven categories, including (1) Field Controller/RTU/PLC/IED, (2) Safety Instrumented System/Protection Relay, (3) Control Server, (4) Data Historian, (5) Human-Machine Interface, (6) Input/Output Server, and (7) Engineering Workstation. Therefore, by considering the metrics shown in Tables 1 and 2, as well as the above categories of components, stakeholders are able to determine the value of likelihood and impact for each and every one of their system components and type of connection, to create a lookup table toward automating the process of computing risk.

[1] https://attack.mitre.org/techniques/ics/.

Table 1 Likelihood [High(H) = 3, Moderate(M) = 2, Low(L) = 1]

Metric	Category	Description	Value
Access vector (AV)	Remote (R)	Remote access to the vulnerable component or link from outside of the system (Internet)	H
	Adjacent (A)	Access to the vulnerable component or link from a neighbor sub-system/sub-network within the same system	M
	Local-physical (LP)	Physical access to the vulnerable component or link from the same sub-system/sub-network in the same system	L
	Local-cyber (LC)	Cyber access to the vulnerable component or link from the same sub-system/sub-network in the same system	M
Required knowledge/skill (KS)	High	A successful attack requires high level of knowledge and skill	L
	Average	An attacker with average level of knowledge/skill can successfully target the vulnerable component or link	M
	None	Accidental failures or blind attacks affect the the vulnerable component or link	H
External factors (EF)	Required	External Factors such as specific windows of opportunity or privileges are required for a successful attack	L
	None	Attack can be conducted at any time without any pre-requirements	H

Table 2 Impact [High(H) = 3, Moderate(M) = 2, Low(L) = 1, None(N) = 0]

Metric	Description	Values
Economic effect (Ec)	Significance of economic loss and/or degradation of products or services	High (H), Moderate (M), Low (L), None (N)
Public effect (P)	Loss of life, medical illness, serious injury, evacuation	High (H), Moderate (M), Low (L), None (N)
Environmental effect (En)	Effect on the public and the surrounding environment	High (H), Moderate (M), Low (L), None (N)
Confidentiality (C)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	
Availability (A)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	
Integrity (I)	Cyber domain (IT assets in a cyber physical system)	High (H), Moderate (M), Low (L), None (N)
	Physical domain (OT assets in a cyber physical system)	

3.4 Rank the importance of identified attack paths

As shown in Fig. 1, for every selected node X_i in phase III, all the unwanted events $\text{UE}_{(X_i)}$ are extracted and then the steps shown in the orange block are repeated to find all the related attack paths and compute the corresponding risk. Noticing the feedback loops in Fig. 1, this process continues to compute the risk associated with all identified critical components. Therefore, once the process in phase III is completed, the result should be ranked and critical components with the higher risk value should be prioritized, so that proper action to reduce or manage the risk is taken. Moreover, for each critical component X_i, the result of computing the cybersecurity risks of pertinent attack paths in Phase III will be listed. Paths with higher risk should be prioritized for each critical component.

Apart from the risk associated with each target component X_i, another factor that can help to manage risk to identify and prioritize attack paths is the *perimeter impact*. According to Table 2, perimeter impact indicates the extent to which a failure/malfunctioning of one node can affect the system and, for instance, cause degradation of products/services or even loss of life. The perimeter impact for each attack path can be computed based on the following equation:

$$\text{P} \cdot \text{Impact}_{\text{path}(i)} = \sum_{i=1}^{n} \text{Impact}_{(X_i)} \tag{7}$$

By analyzing the result of Phase III, we can identify common pre-conditions and components that appear in different attack paths. This will guide us toward breaking down the maximum number of attack paths with less effort; consequently, this improves the security of systems.

Reducing the number of attack paths and breaking an attack path are two actions that can directly reduce the risk.

4 Case study

In this section, we demonstrate the use of our proposed method to assess dependency-based safety and security risk based on the system depicted in Fig. 6. As mentioned earlier, the proposed method is domain-agnostic and can be applied in different domains. To demonstrate that, we showcase the workings of our method using a realistic system with a common ICS architecture that can be found in various domains and encompasses both IT and OT assets. To adapt the ICS part and the architecture of the case study to another domain, one would only need to replace the devices in the field network. First, we describe the system architecture and then apply our method.

4.1 Description

Our case study is developed based on the realistic network infrastructures proposed by Homer et al. [27] and Pan et al. [28]. This system represents a simple approximation of a power system that consists of four network zones: a corporate network, a demilitarized zone (DMZ), a field network, and a control network to control critical infrastructure components in the power system. Like all CPSs, in this case study, the control network connects the supervisory control level to lower-level control modules. The corporate network with the control network allows operators to monitor and control the operations from outside of the field network. The DMZ is a separate network segment that connects directly to the firewall and divides the IT and ICS world, for security reasons. The physical process of the system is carried out in the field network. As illustrated in Fig. 6, the field network in the case study is a three-bus two-line transmission system. It is a modified version of the IEEE nine-bus three-generator system [28] that represents the process of generating and transmitting power to the end users (Load) and includes several components.

G1 and G2 are power generators, BR1 through BR4 are breakers and R1 through R4 are relays. Each relay includes integrated phasor measurement unit (PMU) functionality and is able to trip and open the related breaker when a fault occurs on a transmission line. Operators are also able to manually issue commands to each relay to trip and close the corresponding breaker. The data historian and Human Machine Interface (HMI) are among the key ICS components. The data historian stores the logging of all process information within the ICS while the HMI displays reports and status information regarding the state of the processes under control and enables operators to modify control settings and to configure set points [40].

The DMZ, the web server and the VPN server are accessible from the Internet. The VPN server has access to all hosts except those located in the control network, while the web server has only access to the file server through the NFS file-sharing protocol. Accessing the control network from outside would be only allowed from the Citrix server located inside the corporate network. In this case, the Citrix server can only gain access to the data historian. Operators can send commands to the field devices in the field network from the communication server. Figure 6 also depicts potential locations for the presence of insider attackers in the system.

4.2 Risk analysis

As explained in Sect. 3, the first step to accomplish the dependency-based risk analysis is to collect the required data of the system and model the system (phase I). Therefore,

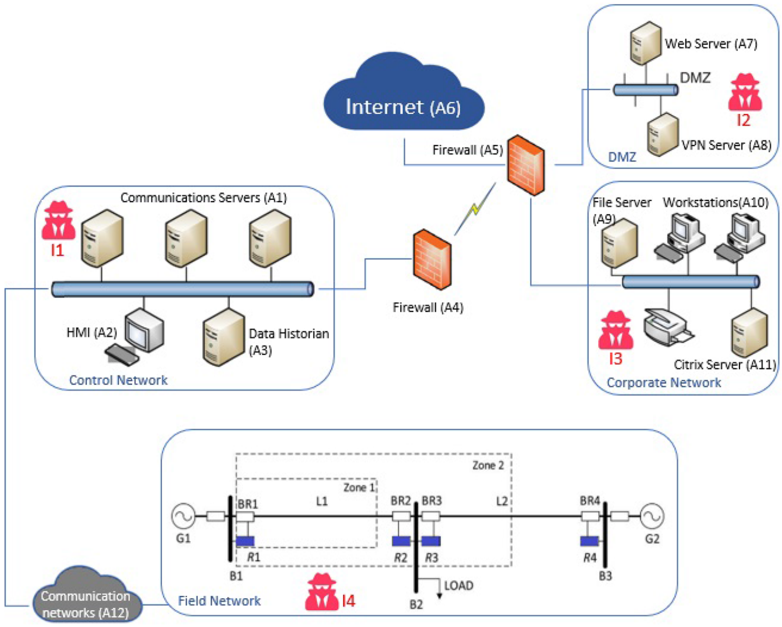


Fig. 6 Graphical representation of the case study

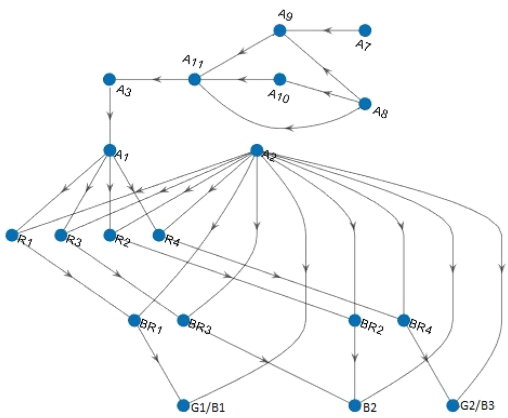


Fig. 7 Digraph of the system

based on the system description and graphical representation of the case study, we provide the digraph of the system as shown in Fig. 7.

Then, we should determine the criticality of the system components following the approach explained in phase II. To this end, the method in [33] is applied to measure the importance of each component from the system level perspective (i.e., C_{sys}). The result of this step is shown in the second column of Table 3. The third column of Table 3 indicates the organizational level criticality of each component which is determined by the expert knowledge here. Finally, by having C_{sys} and C_{Org}, we compute the overall criticality of each component based on Eq. 1 (see Table 3).

According to Table 3, nodes $\{G1, G2, A1, A2, A3, A9, A10, A11\}$ have higher level of criticality compared to other components in the system. Due to the remarkable impact of generators in power systems [38], we select G1 as the target component to run phase III and compute the risk.

Shutting down a generator and damaging it could be seen as two unwanted events. As the former mainly will affect the system, here we choose the latter to investigate how adversaries might be able to cause damage to G1 as one of the system components. Here, we assume that adversaries do not have physical access to G1, as we are interested to analyze the cyber physical attacks and extract related attack paths toward G1. One of the significant reasons that lead to damage to a generator in a power system is the *improper synchronization*.

This could occur due to opening and closing the breaker on the transmission line at a very fast pace which will force the generator to lose synchronization with the transmission grid. When the breaker is opened, the generator is isolated from the grid but due to slow governor response, the mechanical input to the generator does not change immediately. This causes an increase in the generator frequency as compared to the grid frequency. When the breaker is closed out of synchronization or without checking the synchronization requirements, the generator is forced to synchronize; this causes large electrical

Table 3 Criticality value of the system components

Node ID	C_{Sys}	C_{Org}	C_{Total}
B1/G1	0.1693	3	2.1484
BR1	0.357	2	1.6764
R1	0.4916	2	1.811
B2	0.2829	2	1.6023
BR2	0.3423	2	1.6617
R2	0.4761	2	1.7955
BR3	0.3423	2	1.6617
R3	0.4761	2	1.7955
B3/G2	0.1693	3	2.1484
BR4	0.357	2	1.6764
R4	0.4916	2	1.811
A1	1.959	3	3.9381
A2	0.7322	3	2.7113
A3	1.9791	3	3.9582
A7	0.7977	1	1.4574
A8	1.1544	1	1.8141
A9	1.1584	2	2.4778
A10	0.9474	2	2.2668
A11	1.9228	2	3.2422

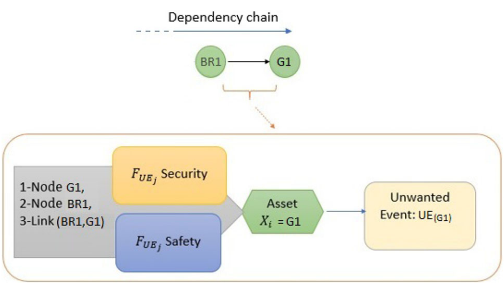


Fig. 8 Checking the first step of the dependency chain for G1

and mechanical transients. The variation of transients due to rapid breaker closing and opening can cause severe physical damage to the generator. Therefore, we consider the improper synchronization as the unwanted event $\text{UE}_{(G1)}$.

Then, we should extract the dependency chains that terminate at G1 and check whether the relations between the nodes in each dependency chain can form attack paths or not. In other words, considering Fig. 4, G1 is placed as the X_i and we investigate the potential cause(s) for $\text{UE}_{(G1)}$ as described in Sect. 3. As shown in Fig. 8, by moving backward from G1, BR1 is the first neighbor node. Considering the functionality of BR1, one can easily find that switching BR1 periodically between the two states, on and off, can lead to the $\text{UE}_{(G1)}$.

Afterward, we consider the attack surface (see Fig. 3) of BR1 to find possible root causes of changing the states of BR1. In the interest of brevity, we only consider the R1 as the neighbor node here. In this case, an intruder (I4) may inject false data into BR1 by leveraging the link $(R1, BR1)$ (this forms path 1 in Table 4), or s/he may take the control of R1 either remotely or manually to send malicious commands to BR1 and change its states between on and off. Path 2 in Table 4 refers to the manual access by I4.

To study the remote access, we should take the next step and identify the attack surface of R1 (i.e., A2 and A1). By following the same approach and leveraging the vulnerabilities described in [27,28], we extract pertinent attack paths that lead to the unwanted event $\text{UE}_{(G1)}$. The results are listed in Table 4. Readers may refer to reference [27] for more details of the vulnerabilities. Note that our main goal here is to show how we can conduct a holistic bottom up risk assessment according to cyber and physical facets of a CPS and available IT/OT knowledge to fill the gap and discover complex cyber physical attacks.

It is noteworthy to heed path 17 in Table 4 as it highlights the necessity of considering both the topological and functional dependencies in risk assessments. As shown in Fig. 6, R1 cooperates in the protection scheme of zone 2 and can trip BR1 when a fault occurs in that zone. Therefore, an attacker may take advantage of this safety scheme to affect G1. In this case, the attacker attempts to emulate a valid fault by sending manipulated data from R3 to the control network and deceive the communication server into sending a trip command to R1 [28,41]. Without considering the functional dependency of A1, this attack path may remain hidden. After identifying the pertinent attack paths, we can determine the likelihood and impact associated with each step of the identified attack paths, based on the guidance in Tables 1 and 2, respectively.

Utilizing a lookup table can facilitate the process of risk assessment. To this end, we develop our lookup table as shown in Table 5. Here, we only consider the components that appear in the identified attack paths. However, in case of a complete risk assessment, this lookup table will be generated for all components, in order to facilitate the computation of likelihood and impact for each system component. Each of the dependency chains shown in Table 5 might appear several times in different attack paths, as will be seen later.

We can then compute the risk and the perimeter impact of each attack path based on Eqs. 2 and 7 as discussed in Sect. 3 (see Table 6). Figure 9 also depicts the risk of each attack path.

As explained in Sect. 3, the risk of $\text{UE}_{(G1)}$ for component $G1$ is computed based on Eq. 3 as follows:

Table 4 Attack paths to G1

No.	Paths
1	$I4 \to BR1 \to G1$
2	$I4 \to R1 \to BR1 \to G1$
3	$A6 \to A7 \to A9 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
4	$A6 \to A8 \to A10 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
5	$A6 \to A8 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
6	$A6 \to A8 \to A9 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
7	$I2 \to A7 \to A9 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
8	$I2 \to A8 \to A10 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
9	$I2 \to A8 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
10	$I2 \to A8 \to A9 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
11	$I3 \to A9 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
12	$I3 \to A10 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
13	$I3 \to A11 \to A3 \to A1 \to R1 \to BR1 \to G1$
14	$I1 \to A1 \to R1 \to BR1 \to G1$
15	$I1 \to HMI \to R1 \to BR1 \to G1$
16	$I1 \to HMI \to BR1 \to G1$
17	$I4 \to R3 \to A1 \to R1 \to BR1 \to G1$

Table 5 Lookup table for Likelihood and Impact of dependency chains

Step	Likelihood	Impact
$A6 \to A7$	AV(H)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A7 \to A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A9 \to A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A11 \to A3$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A3 \to A1$	AV(M)/KS(M)/EF(H)	Ec(L)/P(L)/En(L)/C(H)/A(H)/I(H)
$A1 \to R1$	AV(M)/KS(M)/EF(H)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$R1 \to BR1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(M)/En(M)/C(L)/A(H)/I(H)
$BR1 \to G1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(H)/En(H)/C(M)/A(H)/I(M)
$A6 \to A7$	AV(H)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$A7 \to A10$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(M)/A(M)/I(M)
$A10 \to A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A8 \to A11$	AV(M)/KS(M)/EF(L)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$A8 \to A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I2 \to A7$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$I2 \to A8$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(H)
$I3 \to A9$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I3 \to A10$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(M)/A(M)/I(M)
$I3 \to A11$	AV(M)/KS(M)/EF(H)	Ec(L)/P(N)/En(N)/C(H)/A(M)/I(M)
$I1 \to A1$	AV(M)/KS(M)/EF(H)	Ec(L)/P(L)/En(L)/C(H)/A(H)/I(H)
$I1 \to A2$	AV(L)/KS(M)/EF(H)	Ec(H)/P(H)/En(M)/C(H)/A(H)/I(H)
$A2 \to R1$	AV(M)/KS(M)/EF(L)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$A2 \to BR1$	AV(M)/KS(M)/EF(L)	Ec(H)/P(M)/En(M)/C(L)/A(H)/I(H)
$I4 \to R1/R3$	AV(L)/KS(M)/EF(L)	Ec(M)/P(M)/En(L)/C(M)/A(H)/I(H)
$I4 \to BR1$	AV(L)/KS(M)/EF(H)	Ec(M)/P(M)/En(M)/C(M)/A(H)/I(H)
$R3 \to A1$	AV(M)/KS(M)/EF(L)	Ec(M)/P(M)/En(M)/C(M)/A(M)/I(H)

Table 6 Risk and perimeter impact of identified attack paths

Paths	Likelihood	Perimeter impact	Attack path risk
1	0.0012	0.0723	0.0032
2	0.0013	0.0718	0.0035
3	0.134	0.0659	0.3485
4	0.134	0.0723	0.3485
5	0.0583	0.0723	0.1515
6	0.134	0.0718	0.3485
7	0.1142	0.0659	0.2968
8	0.1142	0.0723	0.2968
9	0.0496	0.0649	0.1291
10	0.1142	0.0645	0.2968
11	0.0496	0.0586	0.1291
12	0.0496	0.0449	0.1291
13	0.0292	0.0488	0.0759
14	0.0055	0.0381	0.0144
15	0.0035	0.0352	0.0092
16	0.0021	0.0244	0.0054
17	0.0053	0.0562	0.0138

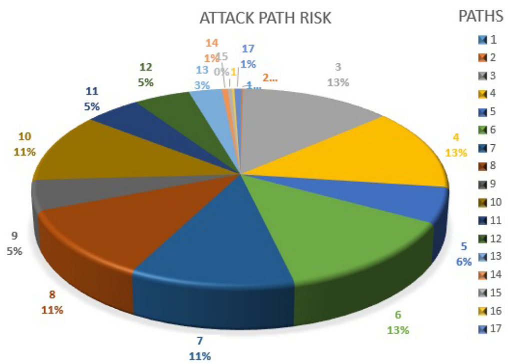


Fig. 9 Risk associated with each attack path

$$
\begin{aligned}
R(G1) &= P(G1) \times \text{Impact}(G1) \\
&= (1 - \prod_{i=1}^{k}(1 - p(\text{path}_i))) \times \text{Impact}(G1) \\
&= (1 - ((1 - 0.0012) \times \cdots \times (1 - 0.0053))) \times 2.6 \\
&= 0.6524 \times 2.6 = 1.6962 \qquad (8)
\end{aligned}
$$

Figure 10 demonstrates the likelihood and perimeter impact of each attack path.

To ensure that the likelihood of each attack path is independent of the length of the dependency chain and the comparison in Fig. 10 is not biased, we divided the value of likelihood of each path by the length of that path (shown in blue color in Fig. 10).

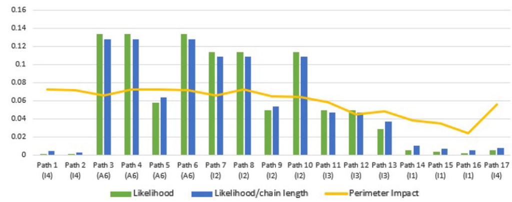


Fig. 10 Likelihood and perimeter impact of identified attack paths

Comparing the identified attack paths based on the likelihood facilitates the identification of the most probable infiltration point and significant attack paths that can lead to the $\text{UE}_{(G1)}$. According to Fig. 10, the likelihood of targeting G1 via A6 and I2 is higher than the rest of the potential entry points. Even within these two groups, the likelihood of path 5 and that of path 9 is significantly low, almost the same as targeting G1 from I3. This information is highly invaluable for risk management in the system.

The advantage of our proposed method will be more clear when it applies to assess the risk of several components in a system. Therefore, we consider relay R1 as the other critical component in the system. In order to calculate the risk of $R1$, we assume that attackers want to modify the settings of relay $R1$. In the system of Fig. 6, relays are configured with a distance protection scheme and changing the settings of a relay can disable the relay function (unwanted event) such that the relay will not trip for a valid fault or a valid command. This can disrupt the smooth operation of the system and cause various types of disturbances in the power system. Attackers can rewrite the settings of a relay either through the HMI on the local network or direct access to the relay. Following the same approach as explained earlier, we extracted the related attack paths to R1 (see Table 7). Then, the likelihood of each path and the impact of targeting $R1$ is calculated and the result is shown in Table 8.

Taking into consideration the identified attack paths, the likelihood and the impact of targeting $R1$, we can compute the risk of targeting $R1$ based on Eq. 3 as follows:

$$
\begin{aligned}
R(R1) &= P(R1) \times \text{Impact}(R1) \\
&= (1 - ((1 - 0.1362) \times \cdots \times (1 - 0.0008))) \times 2.2 \\
&= 0.653 \times 2.2 = 1.4366 \qquad (9)
\end{aligned}
$$

Now, by comparing the risk of $G1$ with that of $R1$ we can clearly understand that, in this system, $G1$ requires higher attention than $R1$ does, which is reasonable as G1 should supply the electrical power to the system. This result is also aligned with the level of criticality of $G1$ in comparison with that of $R1$.

Meanwhile, a closer look at the attack paths in Table 6 reveals that the connections between nodes $A11 \rightarrow A3 \rightarrow$

Table 7 Attack paths to R1

No.	Paths
1	$A6 \to A7 \to A9 \to A11 \to A3 \to A1 \to A2 \to R1$
2	$A6 \to A8 \to A10 \to A11 \to A3 \to A1 \to A2 \to R1$
3	$A6 \to A8 \to A11 \to A3 \to A1 \to A2 \to R1$
4	$A6 \to A8 \to A9 \to A11 \to A3 \to A1 \to A2 \to R1$
5	$I2 \to A7 \to A9 \to A11 \to A3 \to A1 \to A2 \to R1$
6	$I2 \to A8 \to A10 \to A11 \to A3 \to A1 \to A2 \to R1$
7	$I2 \to A8 \to A11 \to A3 \to A1 \to A2 \to R1$
8	$I2 \to A8 \to A9 \to A11 \to A3 \to A1 \to A2 \to R1$
9	$I3 \to A9 \to A11 \to A3 \to A1 \to A2 \to R1$
10	$I3 \to A10 \to A11 \to A3 \to A1 \to A2 \to R1$
11	$I3 \to A11 \to A3 \to A1 \to A2 \to R1$
12	$I1 \to A2 \to R1$
13	$I4 \to R1$

Table 8 Risk and perimeter impact of attack paths toward R1

Paths	Likelihood	Perimeter impact	Attack path risk
1	0.1362	12.6	0.2996
2	0.1362	12.5	0.2996
3	0.0592	1.3	0.1302
4	0.1362	12.6	0.2996
5	0.116	12.6	0.2552
6	0.116	12.5	0.2552
7	0.0504	11.3	0.1109
8	0.116	12.6	0.2552
9	0.0504	11.1	0.1109
10	0.0504	11.1	0.1109
11	0.0297	9.8	0.0653
12	0.0021	5	0.0046
13	0.0008	2.2	0.0018

$A1 \to R1 \to BR1 \to G1$ form the main building block of 11 paths. Notably, the connections between nodes $R1 \to BR1 \to G1$ and $BR1 \to G1$ which appear in another 6 attack paths, are subdivisions of this main building block. This information provides valuable insight for detecting components and corresponding vulnerabilities that frequently appear in different paths; by addressing these, the related attack paths will shrink.

For instance, imagine that we can put in place proper countermeasures to protect the dependency between $BR1$ and $G1$. In this case, none of the identified attack paths can reach $G1$, as adversaries cannot find any vulnerabilities to move from $BR1$ to $G1$ anymore. Although there are still some vulnerabilities and failure modes that attackers can leverage to make their path toward $BR1$, the main goal, i.e., protecting the critical node $G1$, is successfully achieved. Indeed, this satisfies the concept of end-to-end protection that we mentioned earlier, in Sect. 1. Unlike previous risk assessment methods, our proposed method assists system owners and operators to set their objective from the beginning of the analysis and to derive only those paths that can lead to unwanted events affecting the target component. This further helps decision makers to efficiently allocate resources to protect critical components in a system by protecting/removing dependencies existing within the system components that can be leveraged by adversaries to make attack paths toward those critical components.

Here, the risk and the perimeter impact of all attack paths are calculated and these two parameters also help defenders to prioritize the paths with higher risk and impact. In addition to that, the calculation of the overall risk to G1 in case of $\mathrm{UE}_{(G1)}$ facilitates the risk management from a higher level perspective. In other words, while the risk and perimeter impact of each attack path help us to manage the risk associated with a specific unwanted event and its corresponding target component (here $G1$), computing the overall risk of each critical node facilitates the discovery of those unwanted events and pertinent components in a system that require urgent attention and have to be addressed first. Information provided by the proposed risk assessment method can be further utilized to develop a comprehensive risk management method for CPSs; this is part of our future work plans.

5 Discussion

In cyber physical systems, attacks can be carried out from different parts of the system by leveraging flaws and vulnerabilities in cyber components, physical devices, communication links or communication protocols. Therefore, as shown in Sect. 4, discovering and predicting attacks in CPSs require considering both cyber and physical aspects of the systems, as well as the interdependency between them. Considering the physical part of CPSs helps defenders to recognize the intention of attackers and increases the chance of detecting complex cyber physical attacks.

In short, the proposed dependency-based risk assessment has the following characteristics:

- In our proposed method, both the topological and functional dependencies are considered to discover attack paths in a cyber physical system. This means that in the dependency-based risk analysis, the neighbor components with direct connections as well as non-adjacent components that can logically influence the target component due to the functional dependency (i.e., hidden dependency) are studied.
- Unlike previous works which utilize predefined attack vectors and follow a blind investigation to identify target

components in a system, here we apply a backtracking approach which facilitates the exploration of attack scenarios and increases efficiency. This approach also enables operators to view the system from the perspective of attackers and facilitates the detection of new attack paths that might exploit vulnerabilities that have been neglected before and even to discover zero-day vulnerabilities in cyber physical systems.
- Our proposed method is domain-agnostic and can be applied in different CPS domains.
- In our method, the goal of the risk assessment is clear from the beginning, and the risk to each component can be calculated separately. This enhances the efficiency, as unlike previous works, there is no need to investigate the risk of all components/subsystems.
- In this method, risk assessment begins with the most critical components of the system to improve efficiency. To this end, we aggregate the criticality of the system components from both the system and the organizational perspectives.
- By determining the target component corresponding to the unwanted event and moving backwards, the proposed method reduces the investigation of unrelated attack scenarios to zero. That enhances the scalability of the proposed method in comparison with previous ones. The main drawback of the previously developed methods is the speed of growing the number of paths when applied to real-world dimension problems [42] since all the reachable components among the initial components are discovered by moving forward. To extract all attack paths toward a desired component, this process should be repeated for all the components in the system.

6 Conclusion

Unlike previous works, whose main focus has been on the cyber part of CPSs, in this paper both the cyber and physical aspects of a CPS are considered to assess cybersecurity risks. The proposed method facilitates the collaboration between IT and OT operators and, consequently, assists the identification of hard-to-identify and complex attack paths against CPSs. This has been made possible by assessing the risk that the attack paths that lead to a targeted component of a CPS will materialize. Here, an attack path represents violations of security controls that lead to an unwanted event. For every critical component in a system, we extract all the related dependency chains and study potential attack scenarios for each path. For all critical components in a dependency chain, the critical component by itself, its neighbor node, the incoming link are investigated to discover all possible flaws. To increase the efficiency in attack path analysis, a backtracking approach is selected. The workings of the proposed method were showcased using, as an example of a CPS, a realistic power system.

As future work, we plan to present an automated tool to scrutinize possible combinations of vulnerabilities and failure modes of connected components to automatically or semi-automatically generate all attack paths toward target components in a CPS. Besides, the result of the proposed risk assessment method, including the risk and perimeter impact of attack paths, can be further utilized in developing risk management methods for CPSs. We are also interested in studying parallel attack path analysis to investigate its impact on the efficiency of the risk assessment method. The application of the proposed method to CPSs from different domains is also of interest for future work.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital). This work was funded by the Research Council of Norway, through (a) the Joint Indo-Norwegian Project "Cyber-Physical Security in Energy Infrastructure of Smart Cities" (CPSEC), Project No.: 280617; and (b) the SFI "Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS)", Project No.310105.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

1. Alcaraz, C., Lopez, J.: Analysis of requirements for critical control systems. Int. J. Crit. Infrastruct. Prot. **5**(3–4), 137–145 (2012)
2. Abrams, M., Weiss, J.: Malicious control system cyber security attack case study-Maroochy water services, Australia. Tech. Rep, Mitre Corp McLean VA McLean (2008)
3. Chen, T.M., Abu-Nimeh, S.: Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
4. Addeen, H.. H., Xiao, Y., Li, J., Guizani, M.: A survey of cyber-physical attacks and detection methods in smart water distribution systems. IEEE Access **9**, 99 905-99 921 (2021)
5. Castellanos, J. H., Ochoa, M., Zhou, J.: Finding dependencies between cyber-physical domains for security testing of industrial

control systems. In: Proceedings of the 34th Annual Computer Security Applications Conference, pp. 582–594 (2018)
6. Alcaraz, C., Lopez, J., Zhou, J., Roman, R.: Secure SCADA framework for the protection of energy control systems. Concurr. Comput. Pract. Exp. **23**(12), 1431–1442 (2011)
7. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C.: Risk assessment for IoT-enabled cyber-physical systems. In: Advances in Core Computer Science-Based Technologies, pp. 157–173. Springer (2021)
8. Power systems management and associated information exchange—data and communications security—Part 1: Communication network and system security—Introduction to security issues. International Electrotechnical Commission, Geneva, CH, Standard, May (2007)
9. Wang, L., Qu, Z., Li, Z.: The design and implementation of attack path extraction model in power cyber physical system. J. Commun. **11**(9), 834–840 (2016)
10. Chen, Y., Boehm, B., Sheppard, L.: Value driven security threat modeling based on attack path analysis. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), p. 280a. IEEE (2007)
11. Wolf, M., Serpanos, D.N.: Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems. Springer, Berlin (2020)
12. Koscher, K., Savage, S., Roesner, F., Patel, S., Kohno, T., Czeskis, A., McCoy, D., Kantor, B., Anderson, D., Shacham, H.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy, pp. 447–462. IEEE Computer Society (2010)
13. Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., Sztipanovits, J., Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In: 2012 5th International Symposium on Resilient Control Systems, pp. 55–62. IEEE (2012)
14. Shakarian, P.: Stuxnet: Cyberwar Revolution in Military Affairs. Technical Reports, Military Academy West Point NY (2011)
15. Kouns, J., Minoli, D.: Information Technology Risk Management in Enterprise Environments. Wiley, Hoboken (2010)
16. Ali, S., Al Balushi, T., Nadir, Z., Hussain, O.: Risk Management for CPS Security, pp. 11–34. Springer International Publishing AG, Cham (2018)
17. Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique. Requir. Eng. **20**(2), 163–180 (2015)
18. Freund, J., Jones, J.: Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann (2014)
19. Dorofee, C. A. A.: Managing Information Security Risks: The Octave (SM) Approach (2002)
20. Shevchenko, N., Frye, B. R., Woody, C.: Threat modeling for cyber-physical system-of-systems: methods evaluation. In: Carnegie Mellon University Software Engineering Institute Pittsburgh United..., Technical Reports (2018)
21. Kavallieratos, G., Katsikas, S., Gkioulos, V.: Cybersecurity and safety co-engineering of cyberphysical systems-a comprehensive survey. Future Internet **12**(4), 65 (2020)
22. Lamba, V., Šimková, N., Rossi, B.: Recommendations for smart grid security risk management. Cyber-Phys. Syst. **5**(2), 92–118 (2019)
23. Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V.P.: IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. Inf. Secur. **2020**, 1–18 (2020)
24. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K.: A review of cyber security risk assessment methods for SCADA systems. Comput. Sec. **56**, 1–27 (2016)
25. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: Threat and risk assessment methodologies in the automotive domain. Procedia Comput. Sci. **83**, 1288–1294 (2016)
26. Lyu, X., Ding, Y., Yang, S.-H.: Safety and security risk assessment in cyber-physical systems. IET Cyber Phys. Syst. Theory Appl. **4**(3), 221–232 (2019)
27. Homer, J., Varikuti, A., Ou, X., McQueen, M. A.: Improving attack graph visualization through data reduction and attack grouping. In: International Workshop on Visualization for Computer Security, pp. 68–79. Springer (2008)
28. Pan, S., Morris, T., Adhikari, U.: Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. IEEE Trans. Industr. Inf. **11**(3), 650–662 (2015)
29. Krotofil, M., Kursawe, K., Gollmann, D.: Securing industrial control systems. In: Security and Privacy Trends in the Industrial Internet of Things, pp 3–27. Springer (2019)
30. Skopik, F., Smith, P. D.: Smart grid security: Innovative solutions for a modernized grid. Syngress (2015)
31. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.-U.: Complex networks: structure and dynamics. Phys. Rep. **424**(4–5), 175–308 (2006)
32. Akbarzadeh, A., Pandey, P., Katsikas, S.: Cyber-physical interdependencies in power plant systems: a review of cyber security risks. In: 2019 IEEE Conference on Information and Communication Technology, pp 1–6. IEEE (2019)
33. Akbarzadeh, A., Katsikas, S.: Identifying critical components in large scale cyber physical systems. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 230–236 (2020)
34. Bernsmed, K., Frøystad, C., Meland, P. H., Nesheim, D. A., Rødseth, Ø. J.: Visualizing cyber security risks with bow-tie diagrams. In: International Workshop on Graphical Models for Security, pp. 38–56. Springer (2017)
35. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Assessing n-order dependencies between critical infrastructures. Int. J. Crit. Infrastruct. 6 **9**(1–2), 93–110 (2013)
36. Akbarzadeh, A., Katsikas, S.: Identifying and analyzing dependencies in and among complex cyber physical systems. Sensors **21**(5), 1685 (2021)
37. FIRST: Common vulnerability scoring system v3.1: User guide. https://www.first.org/cvss/v3.1/user-guide (2019)
38. Zeller, M.: Myth or reality-does the aurora vulnerability pose a risk to my generator? In: 2011 64th Annual Conference for Protective Relay Engineers, pp. 130–136. IEEE (2011)
39. Zinsmaier, S., Langweg, H., Waldvogel, M.: A practical approach to stakeholder-driven determination of security requirements based on the GDPR and common criteria. In: 6th International Conference on Information Systems Security and Privacy, pp. 473–480 (2020)
40. Stouffer, K., Falco, J., Scarfone, K., et al.: Guide to industrial control systems (ICS) security. NIST Spec. Publ. **800**(82), 16 (2011)
41. Hong, J., Nuqui, R.F., Kondabathini, A., Ishchenko, D., Martin, A.: Cyber attack resilient distance protection and circuit breaker control for digital substations. IEEE Trans. Industr. Inf. **15**(7), 4332–4341 (2018)
42. Hong, J. B., Kim, D. S.: Performance analysis of scalable attack representation models. In: IFIP International Information Security Conference, pp. 330–343. Springer (2013)

11 Article V: Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems[6]

Received 27 February 2022; revised 10 April 2022; accepted 19 May 2022. Date of publication 30 May 2022;
date of current version 9 June 2022. The review of this paper was arranged by Associate Editor Milos Manic.

Digital Object Identifier 10.1109/OJIES.2022.3178834

Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems

AIDA AKBARZADEH AND SOKRATIS KATSIKAS

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2802 Gjovik, Norway

CORRESPONDING AUTHOR: AIDA AKBARZADEH (e-mail: aida.akbarzadeh@ntnu.no).

This work was supported in part by the Research Council of Norway under Project 280617 in the Cyber-Physical Security in Energy Infrastructure of Smart Cities and in part under Project 310105 in the Norwegian Centre for Cybersecurity in Critical Sectors.

ABSTRACT Cyber-Physical Systems (CPSs) engineering profoundly relies on modeling methods to represent the system and study the operation and cybersecurity of CPSs. The operation of a CPS is the result of the collaboration between Information Technology (IT) and Operational Technology (OT) components. While OT focuses on the system's process physics, the emphasis of IT is on information flow. Consequently, different system models are utilized to study various aspects of CPSs, which may infer different views of the same system. The increasing complexity of CPSs and the high number of cyberattacks against Industrial Control Systems (ICSs) and CPSs in recent years have highlighted the necessity of considering these interrelations based on a unified model to analyze cybersecurity of CPSs. However, the diversity of engineering fields and implicit relations and dependencies between them have made it difficult to integrate the modeling methods towards a unified IT&OT model of CPSs.In this paper, we propose a comprehensive method, based on bond graphs, to model CPS and analyze their cybersecurity. Unlike existing methods, modeling the cyber layer along with the physical layer based on the system flow provides a holistic graphical representation of a CPS, which facilitates collaboration between IT and OT experts.

INDEX TERMS Bond graph, cyber physical system, cybersecurity, industrial control system, safety.

I. INTRODUCTION

Cyber-Physical Systems (CPSs) are systems that integrate computation, communication, and controlling capabilities of Information and Communication Technology (ICT), with the traditional infrastructures. This integration facilitates the monitoring and controlling of objects in the physical world as one of the essential requirements of different Critical Infrastructures (CIs), such as manufacturing, healthcare, transportation and the energy sector, to name a few [1], [2]. However, this integration has significantly increased the number of connections among the system components, and this in turn has expanded the attack surface of CIs and has led to making possible complex cyber, and cyber-physical attacks such as Stuxnet and the attacks against the Ukraine's power grid [3]. Cyber-physical attacks have highly increased in recent years in numbers and intensity. For instance, compromising a water treatment facility to poison its community with a ransomware attack against a pipeline operator that disrupted gas supplies to the southeastern United States made the headlines in 2021 [4].

Interactions within a CPS can be classified to cyber–physical, physical–cyber, cyber–cyber, and physical–physical; this also implies that different types of dependency exist in CPSs [5].

As a result, one may attack a CPS in a variety of ways. Nevertheless, not all aspects of cybersecurity in CPSs have received equal attention; the focus has mainly been on information security, protecting access, and ensuring secure delivery of packets, rather than on securing process operations [6], [7].

Bolshev *et al.* argued that following typical security assessments for different CPSs without addressing the cyber–physical/physical–cyber interactions and recognizing the environment in which the system is used will lead to a false sense of security [7]. Recently Krotofil *et al.* showed that a physical process can be leveraged by attackers as a communication medium to deliver malicious payloads between devices that belong to one process in cyber-physical systems, even though these devices are segregated electronically [8].

Their work highlighted the significance of expanding the security scope to cover the physical process layer. Therefore, the analysis of the cybersecurity of a CPS requires an analysis of the cyber components, the physical components, and particularly the interactions between the system components [9]. The authors in [10] provided a list of current research challenges in CPSs and concluded that the essential idea to tackle those challenges is to develop a unified model to capture communication patterns in a high-level that collects the detailed behavior of individual nodes, with respect to different physics and their associate logic. Wang *et al.* also pointed out the importance of understanding the dynamics of various subsystems and their interactions for system designers to develop better CPSs [11].

On the other hand, the diversity of interactions within CPSs also reveals the necessity of collaboration between research communities from different backgrounds, including control theory, power systems, and cyber security, to study associated engineering principles related to the integration of cyber and physical elements of a CPS [12]. In this regard, the IEEE Systems Council established the IEEE Technical Committee on Cyber-Physical Systems in 2017 to promote interdisciplinary research in the design, implementation and operation of CPSs which require the consideration of multiple aspects such as security, reliability, fault tolerance, flexibility and extensibility [13].

Therefore, the security of a CPS highly depends on the collaboration within a cross-functional cybersecurity team that consists of members as suggested in the NIST framework [14]. However, the authors in [15] mentioned that the convergence between Information Technology (IT) and Operational Technology (OT) causes operators to lose a comprehensive understanding of functions and interdependencies within a CPS, and this may lead to incomplete risk assessment. Moreover, IT and OT experts normally utilize different system models, which may infer different views of the same system.

To tackle this challenge, it is required to develop a generic, yet easy to understand model to represent physical and logical facets as well as the interactions within the system components. This will enable both IT and OT experts, and in general members of a cybersecurity team with different backgrounds, to work on the same model and will allow them to identify and predict new complex cyber-physical attacks.

In order to fulfill the aforementioned requirements and to include infrastructures of diverse nature, in this paper we use bond graphs (BGs) to create unified IT&OT models of CPSs. Bond graph is a homogeneous and multi domain modeling approach which has found wide application in the modeling and simulation of physical dynamic systems, due to the physics-based equations derived from it. However, to model a CPS based on the BG approach, it is required to expand the approach to include cyber aspects of CPSs as well. This paper proposes a method that provides a holistic model to study the cybersecurity of CPSs, based on the BG approach. In summary, bond graphs help us to

- Develop a generic and easy to understand multi-domain model of CPSs that represents physical and logical facets as well as the interactions within the system components;
- Achieve a comprehensive understanding of functions and interdependencies within a CPS for both IT and OT experts;
- Facilitate the collaboration within a cross-functional cybersecurity team with people from different backgrounds to analyze the security of CPSs based on the proposed unified IT&OT model.

The rest of this paper is organized as follows: we review the related work on modeling CPSs in Section II. Section III provides the necessary knowledge background of BGs. In Section IV we describe the proposed approach and a case study is leveraged in Section V to demonstrate the application of the method. Finally, Section VI concludes the paper and indicates directions for future work.

II. RELATED WORK

Due to the inherent and ever-growing complexities of CPS, modeling methods are essential to facilitate the representation and analysis of such systems [16]. Indeed, modeling methods simplify the detection of design defects, capturing the evolution of a system, and extracting formal properties, such as determinism, that can be proved later [17].

A complete model of a CPS should indicate a coupling of physical processes, computations and the environment in which the system resides [18]. However, recent literature mainly concentrates on system entities either from the cyber or the physical facets, not of their integration. For instance, Modelica is a multi-domain language for component-oriented modeling of CPSs, which has mainly been developed to model physical systems. Accordingly, although this language has some advantages in modeling the behavior of systems, it cannot accurately cover the interactions between the physical and cyber components within a CPS. Besides, it is hard to understand by a non-expert [19]. The Architecture Analysis & Design Language (AADL) is another modeling language that has been proposed for embedded software systems, which unfortunately cannot support the dynamic physical behavior of the systems [20].

A large number of researchers apply formal methods such as pi-calculus, Petri-net, timed automata and hybrid automata to model CPSs. Formal methods describe the behavior of a system based on the usage of the mathematical specification language. Notwithstanding the capacity of the formal methods to model the physical behavior of complex systems, these methods suffer from high complexity in specifying non-functional properties and providing a visual representation of a system. The authors in [21] stated that formal modeling of CPSs is a complicated and not efficiently executable approach as it includes the double challenge of combined discrete-continuous dynamics and concurrent behavior.

Seiger *et al.* [22] proposed a process-based framework based on Business Process Model and Notation (BPMN). This work shed light on the urgent necessity of representing flows of data within CPS processes from a high-level perspective to assist in understanding the complex behavior of a CPS.

A critical review of different modeling techniques to represent CPSs was conducted in [19]. The authors reviewed 62 papers and stated that, despite the efforts dedicated to modeling CPSs, there are still remarkable open challenges. They concluded that new CPS modeling methods should be developed to a) provide an intuitive and easy to understand multi-domain modeling approach that represents the system processes and targets technical and non-technical stakeholders; b) cover both physical and cyber parts, communication between cyber and physical parts and their corresponding functionalities to portray the behavior of a CPS as a collection of functionalities in the cyber, physical or control part of the system.

Another survey on methods and applications of design and modeling CPSs is provided in [23]. The authors argued that as the development of CPSs deals with challenges from different domains such as mechanics, electronics, engineering, control and computation, it is required to develop transdisciplinary models and conceptual frameworks to integrate them.

Villar *et al.* reviewed different methods and concluded that Model-Driven Engineering is a powerful means to address the increasing complexity of real-time and embedded systems [24]. The authors reached the conclusion that a practical modeling method should be easy to grasp and be applied to different domains and suggested that the number of fundamental modeling primitives should be limited.

Among different graphical modeling methods to represent the physical process of a system, a BG is a description formalism that can be applied in the multidisciplinary dynamic engineering systems from different energy domains such as the mechanical, the electrical, the thermal, and the hydraulic domain [25]. BGs were first used as a modeling tool, and have gradually been extended to solve various challenges, including fault detection and isolation, observability and controllability [26]. Kumar *et al.* [27] presented a method based on the BG modeling approach for modeling a system of systems (SoS). They argued that the causal and structural properties of the BG can be applied to model the control and supervision of a system. Reference [28] utilized the BG model to show the energy interactions throughout a microgrid as a cyber physical system. To verify the accuracy and correctness of the BG model, the author performed a simulation of the microgrid in PLECS and compared it with the BG model. According to this comparison, the author stated that the BG model is a viable approach to model CPSs and to represent their interdisciplinary nature; this approach can be applied in further studies to develop system protection software against cyber attacks. Acknowledging their effort, the main focus of this work is on the energy interactions throughout a microgrid without considering the cyber layer. Zerdazi *et al.* [29] described an approach to model deception attacks on supervisory control and data acquisition (SCADA) systems using BG modeling. The authors argued that an attack on the control signal or sensor measurements can be represented on the BG model by either an additional effort source or flow source.

Considering the previous works, BG is a promising approach to model CPSs, that should expand to cover the cyber layer and the interaction between the cyber and physical components within a CPSs. Expanding the BG model can also contribute to the analysis of different cyber and cyber-physical attacks on CPSs.

Therefore, in this paper, we attempt to a) present a unified IT&OT modeling approach based on the bond graph to capture both physical and cyber characteristics of CPSs to provide better insight; and b) investigate possible faults and cyberattacks by developing a six-step method to enhance the security of CPSs.

III. BACKGROUND

A BG is a graphical representation of a physical dynamic system in the form of a directed graph [30]. A BG is composed of *bonds (edges)* and *elements*. BG modeling is based on the power transfer principle between the different components of a system, since in each energy domain, the amount of power transferred is equal to the product of two physical quantities, i.e, Power = Effort × Flow [31]. Therefore, the physical interaction among components of a system is done by the allocation of Effort (e) and Flow (f) variables on them. Table 1 shows BG variables used in different domains [25].

In a BG, each bond represents the power exchange between the connected elements. In other words, bonds represent the bilateral signal flow of the power-conjugate variables *effort* and *flow*. The symbol of the effort is commonly written above or to the left of a bond and the symbol of the flow below or to the right of that. In BG representation any energetic process can be modeled using the following elements:

- Two *active* elements, sources of effort S_e and flow S_f, which provide input power to the system.
- Three generalized *passive* elements (I, C, and R) of which the R- element represents passive energy dissipation phenomena, while the I- and C- elements represent passive energy storage elements.
- Four *power conserving* elements, namely *transformer (TF)*, *gyrator (GY)*, *flow conservation junction '0'* (is used to regroup BG elements which share the same effort) and *effort conservation junction '1'* (is used to regroup BG elements which share the same flow).
- *Modulated* elements (actuators) whose values depend on some other variables, such as *modulated sources of effort (MSe)* and *modulated sources of flow (MSf)*.
- Two *detectors (sensors)*, namely *detector of effort (De)* and *detector of flow (Df)*, which can measure effort and flow in a system.

For instance, consider an ideal physical model of a simple circuit shown in Fig. 1(a). Here, the circuit is producing power at the voltage source (Ge) and consuming power at the load resistor (R). To model this simple circuit using the BG, we model the voltage source (G_e) and the load resistor (R) with the source of effort *Se* and the R- element, respectively. Since

TABLE 1. Bond Graph Variables in Different Domains [25]

Domain name	Energy	Electronic	Hydraulic	Thermodynamic	Mechanics
First variable	Effort (e)	Voltage (V)	Total pressure (P)	Temperature (T)	Force (F)
Second variable	Flow (f)	Current (I)	Volume flow (Q)	Entropy flow ($S^{\cdot}$)	Velocity (V)

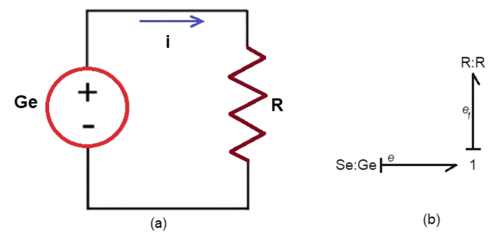


FIGURE 1. (a) A simple circuit with one source and one load. (b) The corresponding BG of the simple circuit.

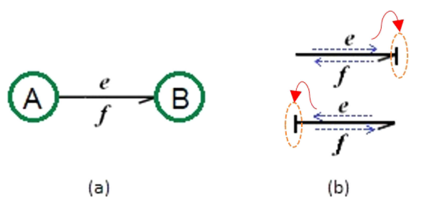


FIGURE 2. (a) The half arrow indicates the direction of the bond, and (b) the causal strokes represent the direction of the effort variable.

G_e is connected in series with R in the circuit, which implies that the same current i flows through both components, we utilize a 1-junction to regroup G_e and R in the BG model, as shown in Fig. 1(b).

A. CAUSAL STROKE

In a BG, a short line perpendicular to the bond at one of its ends is used to represent the (computational) direction of the effort variable *causal stroke*. The causal stroke can lie at either the tip or tail of the half arrow, depending on the causality. The position of the causal stroke is independent of the half arrow that indicates the direction of the bond.

Fig. 2 represents an example of BG modeling in which A and B are two physical elements, and the half-headed arrow is a power bond. The half-arrow, labeled by two unified power variables named effort (e) and flow (f), indicates the exchanged power between A and B. The direction of power flow in a bond is indicated by putting a stroke on the arrow as shown in Fig. 2(b).

Elements in a BG follow different types of causality. S_e and S_f have fixed causality, which means that under any circumstances, only one of the two element variables is allowed to be the outgoing variable. An effort source S_e always supplies effort into the system and has the causal stroke outwards, while a flow source S_f has the dual form of S_e and supplies flow as an input to the system. The C and I elements have a preferred causality, while the R element has an indifferent causality.

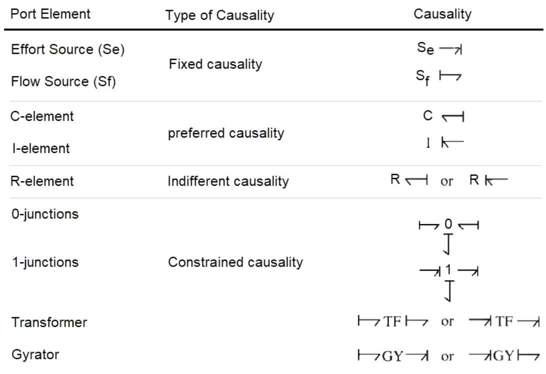


FIGURE 3. Bond graph port elements and their corresponding causality [28].

TF, GY, 0- and 1-junctions have causal constraints relations. Bonds connected to a 0-junction share common effort, and only one bond (i.e., the effort-deciding bond), must bring in the effort. This implies that 0-junctions always have exactly one causal stroke at the side of the junction belonging to the effort-deciding bond. The causal condition at a 1-junction is the dual form of the 0-junction. At a 1-junction, where all flows are the same, only one bond will bring in the flow and has the causal stroke away from the junction. Fig. 3 demonstrates elements and their corresponding causality in a BG.

B. CAUSALITY ASSIGNMENT AND STATE EQUATIONS

Causality assignment or *causal augmentation* is an algorithmic procedure of assigning causality on a BG based on the properties of elements. This process begins with the elements that pose the strongest causality constraints and continues until all elements get their causality assigned. The steps of the process are as follows:

1) Choose an unassigned port with a *fixed causality*, assign its causality, and propagate this assignment through the graph using the causal constraints. Continue this step until all ports with fixed causality are assigned.
2) Choose a not yet causal port with a *preferred causality* (i.e, C- and I-elements), assign the causality, and propagate this assignment through the graph using the causal constraints. Repeat this step until all ports with preferred causality obtain their causalities.
3) Choose a not yet causal port with a *constrained causality*, assign its causality, and propagate this assignment through the graph. Continue this step for all ports with constrained causality.
4) Choose a not yet causal port with an *indifferent causality*, assign its causality, and propagate this assignment

through the graph using the causal constraints. Ensure all ports with indifferent causality received their causality strokes by the end of this step.

A BG model with a correct causality implies that one can extract the set of state equations of the system and compute the unknown variables.

Once the causal strokes are assigned, a BG contains all information necessary to derive the set of state equations describing the system. Depending on the system, the equations are either a set of first-order differential equations (ODEs) or differential-algebraic equations (DAEs). To write the equations, first, each bond on the BG should be labelled to create unique variables. Then, the set of equations will be extracted considering the variable determining the junctions, and unknown variables replaced with the system variables. Notice that BG software like 20-sim [1] automates this process, and there is no need to generate the equations by hand. Nevertheless, we explain how to write equations with an example in Section V. We refer readers to [25], [32] for a detailed description of BG theory and related elements.

IV. THE PROPOSED METHOD

CPSs are governed by various effects of different engineering disciplines and technological components, such as sensors and actuators. Besides, different interactions exist among components within a CPS. For example, the interactions between the cyber part and the physical part in a typical power system [33] are as follows. First, local measurements on a power system sample the voltage magnitudes (or the reactive power outputs of the generators) and convert them into analog or digital signals (physical–cyber interaction). Next, by means of communication networks, this data will be transferred to the control center (cyber–cyber interaction). In the control system, to keep the system in the desired state, pertinent computation will be conducted based on the received data, and appropriate control commands will be sent to the related actuators. Then, these actuators will take proper action based on the received control commands (cyber–physical interaction). Finally, the physical states of the power system will gradually reach the desired point as a consequence of the changes that have been made by actuators (physical–physical interaction). Accordingly, one can understand that the purpose of adding the cyber layer (ICT) to traditional systems is to improve system control and monitoring to ensure that the primary objective of the system, which is delivering a service or commodity to the consumers (end-users), is properly met.

Therefore, we need two types of flow to model CPSs, namely *commodity flow* and *information flow*. Fig. 4 demonstrates the flows and interactions within a CPS.

In the sequel we utilize the flows to describe the physical layer and the cyber layer in CPSs.

[1] https://www.20sim.com/

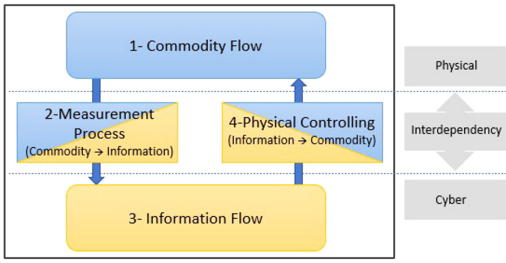


FIGURE 4. Concept model of interactions within a CPS.

A. PHYSICAL LAYER

The commodity flow in a CPS refers to the main objective of the system, i.e. delivering a commodity or service such as electricity, gas, water and oil to the end users. A commodity flow moves from the generator (the initial point) towards the end users of the system and the process physics and the causality of the system could be studied based on that.

As explained in Section I, it was recently shown that attackers might be able to utilize the commodity flow in a CPS as a communication medium to transfer malicious payloads to their target component to affect a system component or disrupt the functionality of the entire system. To this end, the physical layer of CPSs also should be taken into consideration for security analysis. Therefore, we model the physical layer of a CPS based on its objective, main stream of the system, by leveraging the elements of the BG discussed in Section III. This will be further explained with a case study in Section V.

B. CYBER LAYER

In our model, an information flow passes through the cyber components and indicates the interaction among the communication and control parts of the CPSs, i.e. the cyber layer. To address software components as well as other types of low-power devices such as sensors and actuators in the modeling approach, it is necessary to extend our view of the modeling elements presented in the physical layer to include *signals*. In the cyber layer, sensors and actuators are necessary to measure and control the system response and states. Sensors convert a non-electrical signal into an electrical one while actuators perform the opposite. The amount of power that sensors and actuators take out of the system is very small and can be neglected. Therefore, based on the description of energy and effort in the BG approach, the energy transferred by the information flow (electrical signal) is negligible compared to the energy exchanged between the physical components. In the BG approach, information flow is shown as a full arrow on the bond and mainly used to represent the signal transmitted by components such as sensors, actuators and controllers. These system components are said to be *active components* and are represented by a block diagram.

To the best of our knowledge, the information exchange between the active components has been only used to show

FIGURE 5. **Bond graph modeling of: (a) data flow, (b) command signal,(c) data flow with protected channel and (d) command signal with protected channel.**

how system components are connected in a BG, and the mathematical aspect of information flow is neglected insofar it is not related to the physics of the problem. However, information flow in a BG model can be used to study the security of CPSs and turn the BG to a proper approach to conduct a holistic cyber-physical analysis. To this end, we classify the information flow to 1) *data flow*, represented by a full arrow and 2) the *command signal*, represented with a hollow arrow on the bond (see Fig. 5). This will further facilitate the detection of different types of attacks and the investigation of security properties such as the CIA triad, (i.e., Confidentiality, Integrity and Availability) in a CPS. Moreover, channels connecting components in the cyber layer also play a significant role in providing or defeating security. As a result, we expand the BG model to demonstrate the properties of a channel. If a communication channel between two components is protected, this will be indicated with a dashed line, otherwise, it will be represented by a solid line (see Fig. 5). In Fig. 5, A and B are any systems or elements which exchange only information (data or command), and there is no exchange of energy between them. This information bond carries either effort information (effort activated bond with zero flow) or flow information (flow activated bond with zero effort).

C. FAULT AND CYBER ATTACK MODELING

The main focus of OT is on providing the operational safety of the process engineering systems; this is essentially based on fault detection and isolation procedures. These procedures mainly begin with fault modeling, as the most important step, and continue with comparing the actual behavior of the system with the reference behavior. Bond graph is a well known approach to detect faults mainly in the physical layer and has been applied in different domains [26], [34]. In this approach, a fault is modeled as an additional effort source (MSe for 1-junctions) or flow source (MSf for 0-junctions) and added to the same junction where the target element is placed. However, from the cybersecurity perspective, IT is more concerned about the root causes of a fault that occurs in a system, as it might be the consequence of a cyber-attack. Recently, Zerdazi *et al.* [35] used a BG approach to detect deception attacks. Besides, the *Anomaly Detection* methods developed in the cyber domain follow the same approach as for the fault detection in the physical layer. These methods are designed to detect anomalous behavior in a system, based on

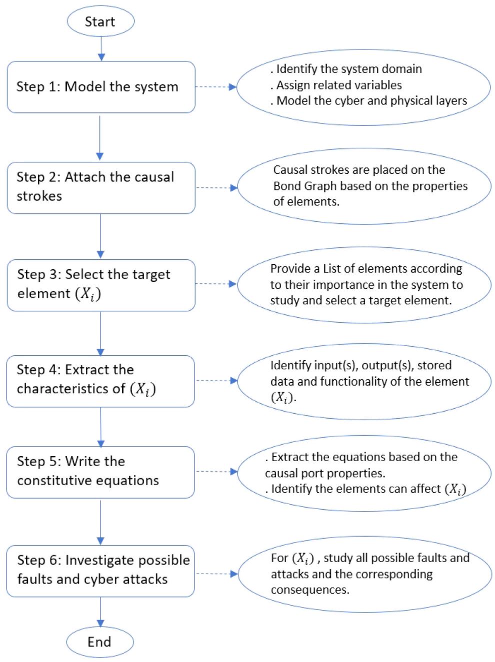


FIGURE 6. **The flow chart of the proposed method.**

the premise that unexpected behavior could be the result of an attack [36]. Considering these two aspects, one can argue that any deviation from the normal values in a CPS is considered a fault; this fault either appears due to influencing the cybersecurity properties (at the cyber layer) or the physical processes (at the physical layer). As a result, utilizing a common model can assist in modeling faults and detecting pertinent causes in CPSs. This can provide better insight and reduce possible conflicts. Therefore, we propose a six-step method based on the BG approach to model a CPS and study possible faults and cyber-attacks. The method is described in the next subsection.

D. METHOD

As shown in Fig. 6, the proposed method consists of the following steps:

Step 1: *Model the system.*

The first step is to identify the domain of the system and the related variables. For example, Fig. 1 shows an electronic circuit, for which we should utilize the pertinent variables *voltage* and *current* (see Table 1). Then, the physical layer of the system and the commodity flow path can be modeled based on the elements presented in Section III. To show the cyber layer, we consider the information flow and model cyber elements and corresponding command and data flows that pass through the system. Notice that properties of the connecting link should also be represented based on the symbols proposed in Fig. 5.

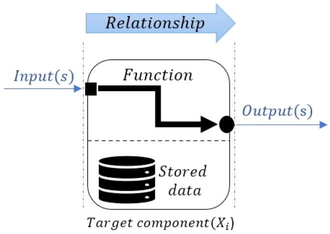


FIGURE 7. Graphical representation of the characteristics of a target element.

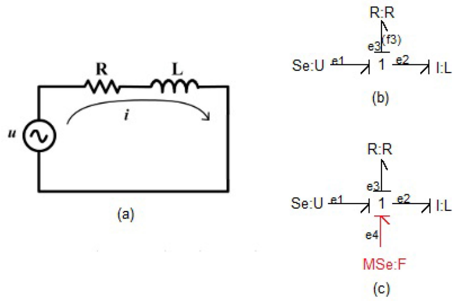


FIGURE 8. (a) A simple RL circuit; (b) the BG model of the RL circuit with the healthy resistance R; and (c) the BG model with faulty resistance, represented by a modulated energy source.

Step 2: *Attach the causal strokes.*

As explained earlier, causal strokes represent the direction of the effort variable, and are required to extract the system equations. Considering the causality assignment procedure described in Section III, the causal strokes should be placed on bonds connected to port elements following this order: first effort and flow sources, then I- and C-elements, followed by transformers and gyrators, and lastly junctions and R-elements. The causality of the rest of the port elements is determined afterwards as they have flexibility in the placement.

Step 3: *Select the target element* (X_i).

Select the system component the analyst is interested in, to investigate possible faults and cyber-attacks. One can provide a list of target elements to check, preferably based on the importance of components in a system. Recently, the authors in [37] proposed a method to rank the criticality of components in CPSs by leveraging the characteristics of system components and their connected links based on the graph metrics, which can be applied here to extract the list of target elements.

Step 4: *Extract the characteristics of the target element.*

This step facilitates the identification of the attack surface for each target element. We enumerate the input(s) and output(s) of the element with respect to their connection properties and extract the functionality of the element. Some elements have stored data like a set point or threshold values to compare with the input; in this case, the stored data also should be considered. Fig. 7 shows the relationship between the input(s) and output(s) of a target element.

Step 5: *Write the constitutive equations.*

For each target element, we write the related constitutive equations based on the causal port properties and substitute the unknown variables as functions of the known variables [38]. Once the equation is derived, we investigate whether variables that appear in the equation can affect the target element in case of the fault occurring, or not. This fault can for example occur due to (accidental) additive noise. For instance, consider the RL circuit shown in Fig. 8. Here, we know that the I-element stores energy and its voltage (e_2) is described by the following equation:

$$e_2 = e_1 - e_3 = U - Rf_3; \quad (e_2 \propto R) \tag{1}$$

As e_2 is proportional to R, a fault on R affects the voltage of the I-element as well. As explained earlier, a fault on R-element can be modeled by a modulated effort source on the 1-junction as depicted in Fig. 8(c) and it changes the value of e_2 by F as (2) shows:

$$e_2 = e_1 + (MSe - e_3) = U + (F - Rf_3); \tag{2}$$

Following the same approach will assist in the identification of values and parameters that can influence the target element, even those elements that are not directly connected to the target element. In the following section, we will discuss this in more detail.

Step 6: *Investigate possible combinations of faults and cyber-attacks.*

Finally, considering the characteristics of the target element explained in step 4 and the identified faults in step 5, we study all possible combinations of faults and attacks for each target element and investigate the corresponding consequences.

V. CASE STUDY: APPLICATION OF PROPOSED METHOD

In this section, we will apply the proposed methodology to detect cyber physical attacks in a typical power system.

Our case study is developed based on the realistic network infrastructures proposed by Pan *et al.* [39]. This system consists of two network zones: a field network, and a control network to control the system. The field network illustrated in Fig. 9 is a three-bus two-line transmission system that is a modified version of the IEEE nine-bus three-generator system [39] and includes several components. G1 and G2 are power generators, L1 and L2 are transmission lines, BR1 through BR4 are circuit breakers and R1 through R4 are relays. Each relay includes integrated phasor measurement unit (PMU) functionality and is able to trip and open the related breaker when a fault occurs on a transmission line. Operators are also able to manually issue commands to each relay to trip and close the corresponding breaker. Fig. 9 also depicts potential locations for the presence of an insider attacker in the system.

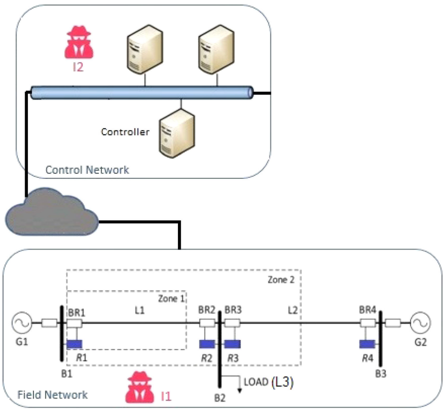


FIGURE 9. **Graphical representation of the case study.**

To investigate possible cyber physical attacks on the power system, we follow the steps proposed in Section IV.

Step 1: To construct the BG model of the case study shown in Fig. 10, we need to determine the appropriate port element of each component in Fig. 9, as explained in Section III. After that, the identified port elements need to be connected using proper port junctions considering the circuit configuration; 1-junction for elements in series and 0-junction for elements in parallel.

Notice that in Fig. 10 the field network is represented in detail to understand the system process; however, for simplicity the controlling part is portrayed in an element called *controller*.

A circuit breaker, which is an electrical switch designed to protect an electrical circuit from damage caused by overcurrent or short circuit, is shown by 1s-junction in the BG model. The 1s-junction represents flow switching and flow will be active at mutually exclusive instants of time. Boolean variables U and $\overline{U}$, are associated with the related bond to model the switching act. For theoretical details, the interested reader may refer to [40]. Fig. 10 shows four 1s-junction with two flow-deciding bonds. As an example, for $1S_1$, when U_1 is 1, flow ($f4$) passes through bond 4 and when $\overline{U_1}$ is 1, $f4$ is 0.

Relays in electrical circuits sense electrical flow and trigger circuit breakers. Accordingly, R1, R2, R3 and R4 in the system are modeled as flow detectors Df (which sense the flow) and modulated source flow MSf (to trigger related circuit breakers). Power generators G1 and G2 are modeled as effort source Se, while load L3 is shown as an R-element. Moreover, the dissipation phenomena on the transmission lines L1 and L2 are modeled by impedance R:L1 and R:L2 in Fig. 10, respectively.

Note that in Fig. 9, elements {G1, BR1, L1, BR2} from the left side and elements {G2, BR4, L2, BR3} from the right side are connected to B2 (Bus2) and are parallel with Load (L3). Therefore, to clearly show these connected components to B2 (Bus2) from both sides and facilitate writing the equations in Step 5, two 1-junctions labelled as $B2$ and $B2'$ are used in the BG model.

Step 2: According to the order of adding causal strokes discussed in Section III-B, we first assign causality to the source elements G1 and G2. Then, we assign the indifferent causality of R-elements {L1, L2, L3}, followed by the constrained causality of the 1-junctions and 1S-junctions. Fig. 10 shows the causal BG of the case study.

Step 3: Here we select R1 as the target element to study its corresponding properties.

Step 4: We extract the characteristics of relay R1 as the target element. A relay (such as R1 in our example) can measure the current that passes through line (L1), and based on the predefined threshold (set-point) or received commands from a controller, controls the associated circuit breaker. Therefore, without loss of generality we can assume that relay R1 is composed of two elements of the BG, one sensor to measure the current and one actuator to trigger the corresponding circuit breakers. It is also possible to model a relay as one mechanical or electrical element based on the BG. However, that would not help us to study the security-related issues in a CPS. It should be noted that the main focus here is to model each element of a CPS in a way that facilitates the analysis of characteristics of the system components and their interactions with other system components, from the cybersecurity perspective. In Fig. 10, Df:R1 denotes the flow detector (sensor), and MSf:T1 refers to the modulated source of flow (actuator).

As shown in Fig. 10, the communication between R1 and its connected elements (circuit breaker and controller) is not protected as there is no protected channel. This is not surprising for communication among elements placed in the field network and the control network in industrial systems.

Therefore, by considering inputs and output of the relay R1, adversaries may inject or replay commands into the relay to change the threshold T1 (i.e., stored data), they may alter or replay sensor measurements (Df) to cause upstream algorithms to take incorrect control actions (controller MQ or R1), or they may alter or replay control commands (from MSf to the breaker) to directly cause incorrect system actions. This can be summarized as follows:

For MSf:T1

Changing the value of T1 via Q12 or manually;

Altering Q12, which consequently will affect the breaker;

Q12:1 Open the breaker (BR1);

Q12:0 Close the breaker (BR1)

Altering Q11 directly;

If $Q11 = 0 \Rightarrow U_1 = 1, \overline{U_1} = 0$ (BR1:Off)

If $Q11 = 1 \Rightarrow U_1 = 0, \overline{U_1} = 1$ (BR1:On)

For Df:R1

Physical attack (fault);

Changing the measured flow value (I_{19});

If $I_{19} < T1 \quad [T1 = Threshold(R1)] \Rightarrow U_1 = 1, \quad \overline{U_1} = 0$ (BR1:Off)

If $I_{19} > T1 \quad [T1 = Threshold(R1)] \Rightarrow U_1 = 0, \quad \overline{U_1} = 1$ (BR1:On)

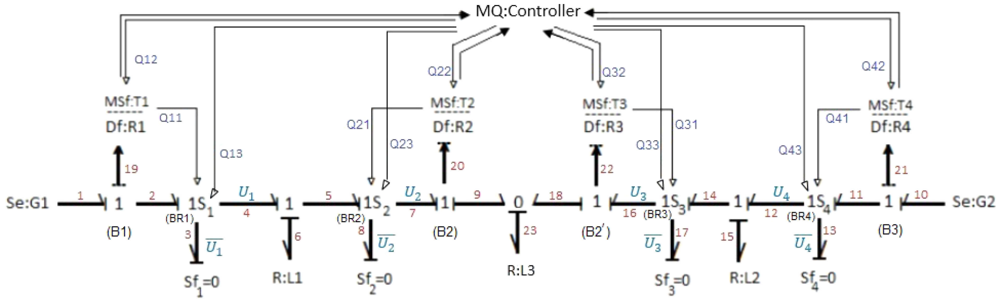


FIGURE 10. **BG model of the case study.**

Step 5: According to the causality shown in Fig. 10 we can write the constitutive equation corresponding to the target element R1. Here, we first extract the equations of all junctions to better understand the system. Considering the rules of the 1-junction in which bonds connected to 1-junction share common flow and the summation of efforts of all bond is zero, we have:

$$f_1 = f_2 = f_{19}, \quad e_1 + e_2 + e_{19} = 0 \tag{3}$$

$$f_4 = f_5 = f_6, \quad e_4 + e_5 + e_6 = 0 \tag{4}$$

$$f_7 = f_9 = f_{20}, \quad e_7 + e_9 + e_{20} = 0 \tag{5}$$

$$f_{16} = f_{22} = f_{18}, \quad e_{16} + e_{22} + e_{18} = 0 \tag{6}$$

$$f_{12} = f_{14} = f_{15}, \quad e_{12} + e_{15} + e_{14} = 0 \tag{7}$$

$$f_{10} = f_{11} = f_{21}, \quad e_{10} + e_{11} + e_{21} = 0 \tag{8}$$

For 1s-junctions we have:

$$f_2 = U_1 f_4 + \overline{U_1} f_3, \quad e_4 = U_1(e_2), \quad e_3 = \overline{U_1}(e_2) \tag{9}$$

$$f_5 = U_2 f_7 + \overline{U_2} f_8, \quad e_7 = U_2(e_5), \quad e_8 = \overline{U_2}(e_5) \tag{10}$$

$$f_{14} = U_3 f_{16} + \overline{U_3} f_{17}, \quad e_{16} = U_3(e_{14}), \quad e_{17} = \overline{U_3}(e_{14}) \tag{11}$$

$$f_{11} = U_4 f_{12} + \overline{U_4} f_{13}, \quad e_{12} = U_4(e_{11}), \quad e_{13} = \overline{U_4}(e_{11}) \tag{12}$$

0-junction is dual of 1-junction. Therefore, we have:

$$e_{18} = e_9 = e_{23}, \quad f_{18} + f_9 + f_{23} = 0 \tag{13}$$

Considering the characteristics of a flow sensor, here e_{19}, e_{20}, e_{22} and e_{21} are equal to zero. Besides, there are two power generators $e1 = G1$ and $e2 = G2$ in the system. For the three resistors {L1, L2, L3} in the system, we have:

$$e_6 = f_6.L1, \quad e_{15} = f_{15}.L2, \quad e_{23} = f_{23}.L3 \tag{14}$$

because, due to Ohm's Law, the current through a resistor (R) is directly proportional to the voltage across the resistor which is represented as $e = f.R$ in the BG.

Now, for the target element R1, we extract the related equation based on (1) to (12) and the causality shown in Fig. 10. Note that the flow measured by the Df:R1 element is I_{19} and $e_{19} = 0$. Therefore, based on the (3) we have:

$$I_{19} = f_2 = f_1; \quad e_2 = -G1 \tag{15}$$

Since f_1 and f_2 are unknown flow variables we should substitute them.

Based on the (9) we have:

$$I_{19} = f_1 = f_2 = f_4 \quad \text{and,} \quad e_4 = e_2 = -G1 \quad (\text{If} \quad U_1 = 1) \tag{16}$$

$$I_{19} = f_1 = f_2 = f_3 \quad \text{and,} \quad e_3 = e_2 = -G1 \quad (\text{If} \quad \overline{U_1} = 1) \tag{17}$$

This approach will be continued until I_{19} can be represented based on known parameters of the system as follows:

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 0 \& U_4 = 0) \tag{18}$$

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 0 \& U_4 = 1) \tag{19}$$

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 0) \tag{20}$$

$$I_{19} = \frac{G1 - I_{21}.L3}{L1 + L3} = \frac{G1}{L1 + L3} + \frac{I_{21}.L3}{L1 + L3} \tag{21}$$

if $(U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 1)$.

For I_{21} we have:

$$I_{21} = \frac{G - I_{19}.L3}{L2 + L3} \tag{22}$$

Therefore, substituting (22) into (21) results in:

$$\begin{aligned} I_{19} &= \frac{G1}{L1 + L3} - \frac{L3}{L1 + L3}\left(\frac{G2 - I_{19}.L3}{L2 + L3}\right) \\ &= \frac{G1(L2 + L3) - L3G2}{(L1 + L3)(L2 + L3) - L3^2} \end{aligned} \tag{23}$$

if $(U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 1)$.

TABLE 2. Relation Between I_{19} and Boolean Variables U

I_{19}	U_1	U_2	U_3	U_4
$I_{19} = \frac{G1}{L1+L3}$	1	1	0	0
$I_{19} = \frac{G1}{L1+L3}$	1	1	0	1
$I_{19} = \frac{G1}{L1+L3}$	1	1	1	0
$I_{19} = \frac{G1(L2+L3)-L3G2}{(L1+L3)(L2+L3)-L3^2}$	1	1	1	1

Equation (23) reveals that the value of I_{19} is dependent on components {L1, L2, L3, G1 and G2} and any change (or fault) of these components directly affects the value of I_{19}. Note that some of these components have a remarkable topological distance from the target element R1.

Step 6: By taking into account the results of step 4 and step 5, here we can investigate different attack scenarios on the target element R1.

In general, relays are placed in the power system to trip the circuit breakers in the case of a fault and overcurrent, to protect transmission lines. Overcurrent protection is critical for personal and system safety from different hazardous conditions that can result from materials igniting. Therefore, it is important to ensure that I_{19} is measured and reported accurately by R1. From step 5, (16), (17), (18) and (21) reveal that the value of I_{19} depends on the Boolean variables U. As a result, an attacker may take advantage of this dependency to attack relay R1 and the system. Table 2 summarizes the relation between I_{19} and the corresponding Boolean variables.

Moreover, the result of step 4 contributes to discovering the following attack scenarios:

- **Trip command injection attacks:** An attacker sends an unexpected relay trip command to relay R1 to open associated breakers. Here, we assume that the attacker aims to trip the breaker BR1 at the ends of transmission line L1 to force L2 to carry more power flow and put the system under stress.
- **Data Injection Attack (or 1LG fault):** In this case, an attacker imitates a valid fault, such as a single line to ground (1LG) fault, by altering the value of (I_{19}). This attack leads to loss of view and may cause an operator to take invalid actions.
- **Relay Disabled Attack**: An attacker changes the settings of relay R1 to disable its operation. As a result, R1 will not trip breakers even in the presence of the pertaining stimulus.
- **Relay setting change Attack**: To disturb the functionality of R1, an attacker changes the stored value of T1 in relay R1 to $T1 + \Delta f$. If $T1 + \Delta f$ is greater than $T1$, then the transmission line L1 experiences over current, which can damage the system and cause safety issues. Likewise, decreasing the threshold (i.e., $T1 + \Delta f < T1$) can cause degradation of service and affect the system performance. However, discovering the latter one is more challenging, and this attack may remain unknown for a while.

To identify more complex attacks, it is required to study both the security properties and the operation of the system in more detail. As an example, consider the Aurora attack in which adversaries send opening and closing commands at a very fast pace to relay R1, to cause the breaker R1 to open and close periodically. This will force the generator G1 to lose synchronization with the transmission line L1 and damage G1 due to stress generated by torque variation.

When an attacker sends the opening command to R1, R1 will trigger BR1, and G1 will be isolated from the grid. The attacker knows that because of the slow governor action, the generator can not stop immediately and its frequency will keep increasing. This leads to a frequency difference between the grid and the generator G1. Therefore, the attacker leverages this vulnerability and sends a closing command to R1 at a very fast pace (before 15 cycles) to connect G1 to the grid with "out-of-sync" conditions. This causes large electrical and mechanical transients, damage to G1, and even blackout. It is clear that discovering and conducting the Aurora attack, as an example of a complex attack in CPSs, mainly depends on proper knowledge of the process physics of the system.

Notice that, due to the nature of a power conserving description of a system in the BG, one can model the generator G1 based on its electromechanical properties to investigate the effect of improper synchronization in this example. Indeed, this implies the *reusability* of modeling CPSs based on the BG, which is a valuable advantage in modeling the systems that cover several physical domains, and those systems might need to be expanded/modified later [24].

As the last point, this approach can also contribute to sensitivity analysis of the interactions and system components in case of faults and attacks. For instance, a closer look at (16), (17) and (18) shows that I_{19} is equal to $\frac{G1}{L1+L3}$ if at least one of the $U3$ and $U4$ is zero. This implies that not all deviations and parameter changes have an equal impact on the system.

VI. CONCLUSION

In this paper, we showed that modeling the cyber layer along with the physical layer based on the system flow, as the initial target of a CPS, can provide a holistic view of a CPS and allow to evaluate how adversaries might perturb the cyber part and ultimately the physical part of the system. To the best of our knowledge, none of the available methods reviewed in section II provides this. Accordingly, we proposed a comprehensive and domain-agnostic method, based on the BG approach. According to the proposed six-step method, one can follow the sequence of interactions based on the topological parts of the model and utilize corresponding equations to investigate dependencies and relations between the components of a CPS to extract potential fault points, attack surfaces, and the consequences of attacks. Considering the numerous components of large-scale CPSs, this investigation begins with the most critical components ranked in the list of target components that contribute to the optimization of the analysis. Modeling a CPS based on its fundamental object that represents the process physics of the system along with the cyber layer will help operators and the security team to discover potential complex attacks. As stated in [17], modeling methods simplify the detection of design defects; this can also assist system designers and operators to examine what-if design scenarios and enhance the security and fault tolerance of CPSs by applying proper countermeasures at early stages. Additionally, in modeling large systems, reusability is a critical feature; as shown in the case study, the proposed approach has this capability for different physical domains. Therefore, in case of any changes in the system, its model can be easily modified. Developing software tools for supporting the full application of the proposed method and demonstrating its applicability and usefulness in further realistic examples of a larger scale is among our future research plans.

REFERENCES

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

[2] T. Tagarev, N. Stoianov, and G. Sharkov, "Integrative approach to understand vulnerabilities and enhance the security of cyber-bio-cognitive-physical systems," in *Proc. Eur. Conf. Cyber Warfare Secur.*, 2019, pp. 492–XIX.

[3] A. Cardenas and S. Cruz, "Cyber-physical systems security knowledge area," in *Proc. Cyber Secur. Body Knowl.*, pp. 3–9, 2019.

[4] DRAGOS, "ICS/OT cybersecurity year in review 2021," pp. 4–5, 2022. [Online]. Available: https://hub.dragos.com/report/2021-year-in-review

[5] A. Akbarzadeh and S. Katsikas, "Identifying and analyzing dependencies in and among complex cyber physical systems," *Sensors*, vol. 21, no. 5, 2021, Art. no. 1685.

[6] C. Bodei, P. Degano, G.-L. Ferrari, and L. Galletta, "Tracing where IoT data are collected and aggregated," *Log. Methods Comput. Sci.*, vol. 13, no. 3, Jul. 2017, doi: 10.23638/LMCS-13(3:5)2017.

[7] A. Bolshev, J. Larsen, M. Krotofil, and R. Wightman, "A rising tide: Design exploits in industrial control systems," in *Proc. 10th USENIX Workshop Offensive Technol.*, 2016, pp. 178–188.

[8] M. Krotofil, K. Kursawe, and D. Gollmann, "Securing industrial control systems," in *Security and Privacy Trends in the Industrial Internet of Things*. Berlin, Germany: Springer, 2019, pp. 3–27.

[9] R. Akella, H. Tang, and B. M. McMillin, "Analysis of information flow security in cyber–physical systems," *Int. J. Crit. Infrastructure Protection*, vol. 3, no. 3/4, pp. 157–173, 2010.

[10] P. Sobhrajan, S. Y. Nikam, D. Pimpri, and P. D. Pimpri, "Comparative study of abstraction in cyber physical system," *Int. J. Comput. Sci. Inf. Technol*, vol. 5, no. 1, pp. 466–469, 2014.

[11] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Convers. Econ.*, vol. 2, pp. 197–211, 2021.

[12] J. Butts, M. Rice, and S. Shenoi, "Modeling control system failures and attacks–the Waterloo campaign to oil pipelines," in *Proc. Int. Conf. Crit. Infrastructure Protection*, 2010, pp. 43–62.

[13] S. Hu and A. Y. Zomaya, *IEEE Tech. Committee Cyber-Physical Syst. (CPS)*, [Online]. Available: https://ieeesystemscouncil.org/cyber-physical-systems-technical-committee

[14] K. Stouffer *et al.*, "Guide to industrial control systems (ICS) security," *NIST Special Publication*, vol. 800, no. 82, pp. 16–16, 2011.

[15] B. Green, M. Krotofil, and D. Hutchison, "Achieving ICS resilience and security through granular data flow management," in *Proc. 2nd ACM Workshop Cyber- Phys. Syst. Secur. Privacy*, 2016, pp. 93–101.

[16] S. J. Oks, M. Jalowski, A. Fritzsche, and K. M. Möslein, "Cyber-physical modeling and simulation: A reference architecture for designing demonstrators for industrial cyber-physical systems," *Procedia CIRP*, vol. 84, pp. 257–264, 2019.

[17] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[18] J. C. Jensen, D. H. Chang, and E. A. Lee, "A model-based design methodology for cyber-physical systems," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, 2011, pp. 1666–1671.

[19] I. Graja, S. Kallel, N. Guermouche, S. Cheikhrouhou, and A. Hadj Kacem, "A comprehensive survey on modeling of cyber-physical systems," *Concurrency Comput.: Pract. Experience*, vol. 32, no. 15, 2020, Art. no. e4850.

[20] Z. Yu, D. Yunwei, Z. Fan, and Z. Yunfeng, "Research on modeling and analysis of CPS," in *Proc. Int. Conf. Auton. Trusted Comput.*, 2011, pp. 92–105.

[21] E. Kamburjan, S. Mitsch, M. Kettenbach, and R. Hähnle, "Modeling and verifying cyber-physical systems with hybrid active objects," Jun. 2019, *arXiv:1906.05704*.

[22] R. Seiger, S. Huber, and T. Schlegel, "Toward an execution system for self-healing workflows in cyber-physical systems," *Softw. Syst. Model.*, vol. 17, no. 2, pp. 551–572, 2018.

[23] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama, and S. Achiche, "Design, modelling, simulation and integration of cyber physical systems: Methods and applications," *Comput. Ind.*, vol. 82, pp. 273–289, 2016.

[24] E. Villar, J. Merino, H. Posadas, R. Henia, and L. Rioux, "Mega-modeling of complex, distributed, heterogeneous CPS systems," *Microprocessors Microsystems*, vol. 78, 2020, Art. no. 103244.

[25] W. Borutzky, *Bond Graph Methodology: Development and Analysis of Multidisciplinary Dynamic System Models*. Berlin, Germany: Springer, 2009.

[26] S. Benmoussa, B. O. Bouamama, and R. Merzouki, "Bond graph approach for plant fault detection and isolation: Application to intelligent autonomous vehicle," *IEEE Trans. Automat. Sci. Eng.*, vol. 11, no. 2, pp. 585–593, Apr. 2014.

[27] P. Kumar, R. Merzouki, B. O. Bouamama, and A. Koubeissi, "Bond graph modeling of a class of system of systems," in *Proc. 10th Syst. Syst. Eng. Conf.*, 2015, pp. 280–285.

[28] M. J. White, "Bond graph modeling of critical infrastructures for cyber-physical security implementation," Ph.D. dissertation, Dept. Elect., Missouri Univ. Sci. Technol, Rolla, MO, USA, 2021.

[29] I. Zerdazi and M. Fezari, "Scada attack modeling using bond graph," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manage.*, 2019, pp. 1–2.

[30] W. Borutzky, *Bond Graph Modelling of Engineering Systems*, vol. 103. Berlin, Germany: Springer, 2011.

[31] P. Carreira, V. Amaral, and H. Vangheluwe, *Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems*. Berlin, Germany: Springer Nature, 2020.

[32] R. Merzouki, A. K. Samantaray, P. M. Pathak, and B. O. Bouamama, *Intelligent Mechatronic Systems: Modeling, Control and Diagnosis*. Berlin, Germany: Springer Science & Business Media, 2012.

[33] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[34] M. Yu, C. Xiao, W. Jiang, S. Yang, and H. Wang, "Fault diagnosis for electromechanical system via extended analytical redundancy relations," *IEEE Trans. Ind. Inform.*, vol. 14, no. 12, pp. 5233–5244, Dec. 2018.

[35] I. Zerdazi, M. Fezari, and M. Ouziala, "Detection of deception attacks in supervisory control systems using bond graph," *Autom. Control Comput. Sci.*, vol. 54, no. 2, pp. 156–167, 2020.

[36] E. D. Knapp and J. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Amsterdam, Netherlands: Syngress, 2014.

[37] A. Akbarzadeh and S. Katsikas, "Identifying critical components in large scale cyber physical systems," in *Proc. IEEE/ACM 42nd Int. Conf. Softw. Eng. Workshops*, 2020, pp. 230–236.

[38] B. O. Bouamama, A. Samantaray, K. Medjaher, M. Staroswiecki, and G. Dauphin-Tanguy, "Model builder using functional and bond graph tools for FDI design," *Control Eng. Pract.*, vol. 13, no. 7, pp. 875–891, 2005.

[39] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Trans. Ind. Inform.*, vol. 11, no. 3, pp. 650–662, Jun. 2015.

[40] A. C. Umarikar and L. Umanand, "Modelling of switching systems in bond graphs using the concept of switched power junctions," *J. Franklin Inst.*, vol. 342, no. 2, pp. 131–147, Mar. 2005.

12 Article VI: Towards Comprehensive Modeling of CPSs to Discover and Study Interdependencies [7]

Towards Comprehensive Modeling of CPSs to Discover and Study Interdependencies *

Aida Akbarzadeh[0000−0002−3142−1583] and Sokratis Katsikas[0000−0003−2966−9683]

Norwegian University of Science and Technology, Gjøvik, Norway
aida.akbarzadeh@ntnu.no, sokratis.katsikas@ntnu.no

Abstract. To a large extent, modeling Cyber-Physical systems (CPSs) and interdependency analysis collaborate in the security enhancement of CPSs and form the basis of various research domains such as risk propagation, attack path analysis, reliability analysis, robustness evaluation, and fault identification. Interdependency analysis as well as modeling of interdependent systems such as CPSs rely on the understanding of system dynamics and flows. Despite the major efforts, previously developed methods could not provide the required knowledge as they have either followed data-driven or physics-based modeling approaches. To fill this gap, we propose a new modeling approach called BG2 based on Graph theory and Bond graph. Our proposed method is able to portray the physical process of CPSs from different domains and capture both information and commodity flows. Based on the fundamental characteristics of the Graph theory and Bond graph in the BG2 model, we discover higher order of dependencies in CPSs and analyze causal relationships within the system components. We illustrate the workings of the proposed method by applying it to a realistic case study of a CPS in the energy domain. The results provide valuable insight into the dependencies among the system components and substantiate the applicability of the proposed method in modeling and analyzing interdependent systems.

Keywords: Interdepedency Analysis · CPS Modeling · Cyber-Physical systems · Bond Graph · Graph Theory · Security.

1 Introduction

Cyber-Physical Systems (CPSs) integrate computation, communication, and control capabilities of Information and Communication Technology (ICT) into physical objects and traditional infrastructures to facilitate the monitoring and controlling of objects in the physical world. Based on the NIST framework for cyber-physical systems, a CPS can be seen as an individual block or as a system

* This work was supported by the Research Council of Norway under project 280617 (Cyber-Physical Security in Energy Infrastructure of Smart Cities - CPSEC) and under project 310105 (Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS)

of systems (SoS) that encompasses multiple subsystems with several heterogeneous parameters [17]. It is worth mentioning that CPSs are the building blocks of Critical Infrastructures (CIs) which are essential for the maintenance of vital societal functions, such as manufacturing, healthcare, transportation, and the energy sector [8, 38].

In a CPS, as a system of systems, individual parts work collectively to accomplish the main objective of the system, and the service provided by the system is actually formed based on the behavior of all constitutive parts and interactions among them. That also implies that the functionality and security of a CPS depend on each constitutive part and the relationship among them. Indeed, each part has its own characteristic and may react differently in case of an unexpected situation like a cyber attack. Any failure or malfunction in an individual part not only can affect the functionality of the part itself but also may influence the dependent parts and the entire system. The electric power disruption in California [35], the attack on Florida water treatment plant [2] and the Maroochy attack [1] are examples of failures and cyber attacks which initiated at an individual part but significantly affected the entire system. Therefore, researchers in many domains attempt to develop appropriate methods to model Cyber Physical systems with an eye to studying underlying relations and dependencies between the components of a CPS. Identification of these dependencies in a CPS provides an insightful view of cause and effect relationships, failure types, response behavior, state of operation, and risks to the system [23, 29]. For this reason, dependency analysis is an underlying basis for various research domains such as reliability analysis [27], robustness evaluation [14] and failure propagation [46] to name a few.

Significant efforts have been dedicated to modeling and analysis of CPSs and their interactions, particularly in recent years. These proposed methods were mainly developed based on Graph theory [47], Input-Output Models [39], Bayesian networks, Petri nets [26], Agent-Based Models, and Multi-Agent Modelling [43] and differ broadly according to the granularity, details, and level of abstraction applied. Jensen et al. explained that a comprehensive model of a CPS should portray the coupling of physical processes and computations in the system by considering the environment in which the system resides [21]. Nevertheless, the main focus of previously developed methods dedicated to model CPSs as disjoint services/layers, and the interactions within a CPS and heterogeneity of these interactions gained fewer attention [11]. Considering these modeling requirements for CPSs as well as the heterogeneous components and their interactions in a system, Khaitan argued that the current modeling approaches and frameworks are inadequate [22].

The concurrency of different physical and computational processes as well as the heterogeneous nature of CPSs turn the CPS modeling into a complex task. Zhang et al. [46] mentioned that current literature is lacking approaches that can capture the engineering aspects of interdependent networks. The authors in [27] also pointed to the differences between the physical and cyber facets in a CPS and highlighted the lack of interdependent system modeling in literature to portray these fundamental differences. That becomes more critical when system modeling aims to study the security of CPSs. We have recently witnessed sophisticated cyber-physical attacks such as Stuxnet [13] and the Florida water plant attack [2] that revealed the necessity of dependency analysis in CPSs more than ever. Considering the concept of "kill chain" which describes an attack as a step-by-step approach [45], the authors in [5] stated that each attack (or attack path) refers to a "chain of dependency" in a system that has been successfully materialized by attackers. Krotofil et al. showed that the physical process layer should be included in system modeling in the security scope as the physical process can be utilized as a communication medium to deliver malicious payloads between system components [24]. Furthermore, the multidisciplinary nature of CPSs is another factor that an ideal system modeling should be capable of addressing to provide a deeper understanding of interdependencies and their implications for system security [34]. Among different modeling methods, our research showed that Bond graph (BG) has the capability of providing the aforementioned requirements. Bond graph is a description formalism that can portray the physical process of a system based on the flows of system commodities from different energy domains such as the electrical, mechanical, mechatronics, chemical, hydraulic, and thermal as well as multidisciplinary dynamic engineering systems [10]. Additionally, the BG diagram can represent the causality between system elements that contributes to the formulation of system equations and investigation of the system behavior in terms of controllability, observability, and fault diagnosis [9]. These characteristics of Bond graph turn it into an ideal method for modeling the physical processes of CPSs and analyzing dependencies between the system components. Moreover, reviewing recent interdependency studies showed us that Graph theory, as the most common underlying method applied for dependency analysis in complex systems, has significant features for modeling and analyzing the cyber part of CPSs which performs the controlling and monitoring tasks [7, 37, 41]. Therefore, in order to fill the gap found in the literature for modeling CPSs and interdependency study as a basis of various research domains, in particular, for the cybersecurity domain, we attempt to develop a new method based on merging Bond graph and Graph theory. Based on the proposed method, we will not only be able of extracting dependencies in CPSs, but also we can study the cause and effect relationship between the system components. Our main contribution is twofold:

- We develop a novel method, called BG2 model, based on Graph theory and Bond graph for modeling cyber-physical systems considering the multidisciplinary nature of such systems, and
- we apply the proposed BG2 model to discover and analyze dependencies and causal relationships within the system components in a CPS.

The remaining of the paper is structured as follows: Section 2 reviews the related work on modeling CPSs and dependency analysis. Section 3 provides the necessary knowledge background of Graph theory and Bond graph. We describe the proposed method in section 4, and a case study to expound on the application of the proposed method is presented in section 5. Finally, section 6 summarizes our findings and indicates possible future work.

2 Related work

A survey conducted by Hehenberger et al. on methods and applications of modeling CPSs revealed the necessity of developing transdisciplinary models and conceptual frameworks to encompass attributes of CPSs stem from different domains such as electronics, mechanics, engineering, and control [18]. Rinaldi et al. also reviewed pertinent approaches for modeling and simulating CIs and their interdependencies and concluded that the multidisciplinary science of interdependent systems such as CPSs which consists of multiple disciplines is relatively immature [34]. To address this challenge, recently Akbarzadeh et al. proposed a unified IT&OT modeling approach based on Bond graph to model CPSs, facilitate collaboration between IT and OT experts, and discover the attack surface of system components with the goal of improving cybersecurity of CPSs. Their work showed Bond graph as a promising basis for modeling CPSs and analyzing their dependencies, particularly for the physical process of the systems. Bond graph is an explicit graphical model for capturing and representing the common energy structure of systems. Besides, one can apply the causal and structural properties of BGs to study systems' behavior. Kumar et al. utilized Bond graph to model a system of systems (SoS) [25], while other researchers applied BG as a homogeneous and multi-domain modeling approach to study fault detection and isolation, observability, and controllability in complex systems [9, 44].
Interdependency analysis in CPSs contributes to assessing the consequences of failures occurrence and failures propagations in a system. Moreover, this helps to understand how failures can disturb the functionality of a CPS and consequently affect the reliability of the system. As a result, modeling CPSs with the aim of interdependency analysis provides an insightful view of inter-system and intra-system causal relationships, response behaviors, failure types, state of operations, and risks the systems might encounter [23, 29]. Besides, interdependency modeling and studying the systems' behaviors in the presence of failures is a common approach to evaluating the security and reliability of CPSs, as these failures may be caused by adversaries [33, 15].
Rinaldi et al. proposed six dimensions of infrastructure interdependencies namely, type of failure, coupling and response behavior, infrastructure characteristics, environment, types of interdependencies, and state of operation to study dependencies in CIs [34]. In the follow-up paper [34], the same authors highlighted the necessity of developing interdependency analysis capabilities and improving information integration in modeling and simulation methods to protect CIs. The authors mentioned that these objectives are also aligned with the homeland security programs and can provide insights into rare events like complex cyber-physical attacks [20].
Satumtira et al. [37] surveyed 162 papers on interdependency modeling and discovered that Graph theory is the most common method to study interdependen-

cies in CIs. later on, Torres [41] compared different methods applied for modeling CIs including Agent-based Models, Petri Nets, Bayesian Networks, and Graph theory based on six different objectives namely *Scalability*, *CPU time*, *Usability*, *Tools accessibility*, *Dynamic simulation* and *Large systems modeling*. Their evaluation confirmed the capacity of Graph theory as the most suitable method found in the literature to study CPSs, as Graph theory gained the highest value in four out of six different objectives in the comparison. Recently, the authors in [4] proposed the Modified Dependency Structure Matrix (MDSM) based on Graph theory to identify, illustrate and evaluate the quantitative characteristics of connections, including multi-order dependencies, in large-scale CPSs. Nevertheless, the Graph theory-based approaches mainly provide a high-level perspective of CPSs with an emphasis on the topological characteristics of the systems. In our previous paper, we reviewed and compared recent graph-based interdependency analysis methods in the power domain based on different features including the *communication direction*, *applied control parameters*, *system functionality*, *system security*, *complexity* and *scalability*, and the results showed us there are still remarkable open challenges require to address [7]. Graja et al. also conducted a critical review of different modeling and analysis techniques found in 62 papers and stated that despite significant efforts, current research is still at the beginning stage [16]. In a nutshell, dependency analysis as a basis for various research fields requires a paradigm shift from a disjoint modeling approach to transdisciplinary models that enables to capture of the physical processes in lower levels, the monitoring and controlling of the cyber part as well as the communication between cyber and physical parts and their corresponding functionalities in a CPS to portray the behavior of a CPS as a collection of functionalities from different domains. This paves the way towards causality analysis in complex systems and contributes highly to improving the security of such systems [16, 11, 28, 44].

3 Background

In this section, a brief overview of Graph theory and Bond graph is given.

3.1 Graph Theory

A graph is a mathematical representation of a network. A network can be modeled as a graph $G(V, E)$ where V is a set of vertices and E is a set of links [31]. A vertex (node) V is an intersection point of a graph and can denote a component of a system, while an edge (link) E is a link between two nodes. $V(G)$ and $E(G)$ are referred to as the *vertex (node) set* and the *edge (link) set* of graph G, respectively. Graphs can be *Directed* or *Undirected*. If the direction of each edge is defined in a graph, that is a directed graph. Otherwise, it is known as an undirected graph. In Graph theory, a directed graph D is a pair (V, E) where E is a subset of $V \times V \equiv \{(x, x)|x \in V\}$ and $(u, v) \in E$ implies that there is an edge e which joins the initial node (tail) u to its terminal node (head) v [40].

In graph G, the *Indegree Centrality* shows the number of links that enter each node, while the *Outdegree Centrality* refers to the total number of outgoing links from each node. Graph theory is the study of the relationship between edges and vertices and can be applied to any scenarios that aim to examine the structure of a network of connected objects.

3.2 Bond Graph

A Bond graph is a graphical representation of a physical dynamic system based on the energy exchange phenomenon between the system components. Due to the fact that in each energy domain, the amount of power transferred equals the product of two physical quantities, i.e, Power = Effort × Flow, Bond graph provides a uniform notation for modeling dynamic systems from different domains such as electrical, hydraulic and mechanical as well as multi-domain dynamic systems [12]. For instance in electrical domain power exchange is computed based on the *Voltage* (V) and *Current* (I) while in the hydraulic domain the two physical quantities utilized to compute power are *Pressure* (ρ) and *Volume Flow Rate* (Q). Bond graph is composed of *bonds (edges)* and *port elements*. Bonds connect port elements and portray the direction of power flow by half arrows while the two power conjugated variables named *effort (e)* and *flow (f)* are assigned to each bond. Port elements indicate how energy exchanges across bonds based on the underlying physics principles in which energy can convert into another energy form, transform in the same energy domain, transfer from one power port to another, be distributed, or be stored [10]. Figure 1 shows port elements and their corresponding causality in the Bond graph.

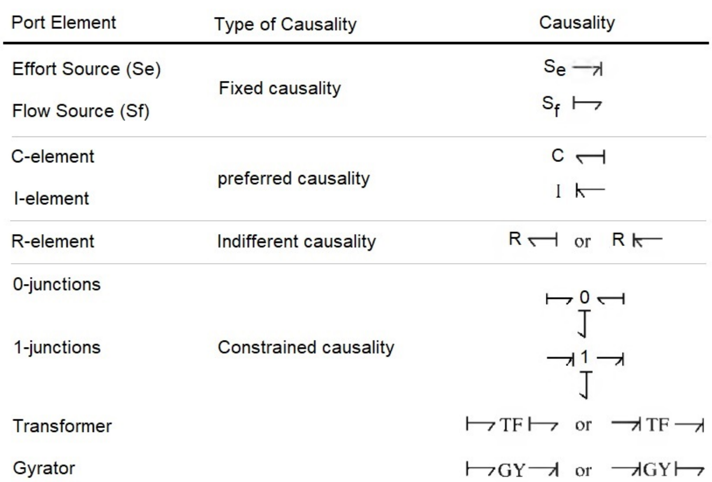


Fig. 1. Bond graph port elements and their corresponding causality [6].

One of the main advantages of BG modeling is its capability to study the characteristics of causality in a system. This facilitates the analysis of interactions and cause-effect relationships between the system components, as well as the structural analysis of systems such as controllability and observability.
Causal stroke: In BG diagrams, a *causal stroke* shows the direction of imposing effort (e) and represents by a short line perpendicular to the bond at one of its ends, either the tip or tail of the half arrow. Notice that the causal stroke is independent of the power transfer direction shown by the half arrow. In Bond graph when one side causes effort, the other side causes flow and the causal stroke is placed near the element for which the effort is known [30]. For instance, in figure 2-(a), X imposes the effort (e) to Y, i.e effort (e) is known for Y, whose effect sets the flow (f) towards X. Figure 2-(b) shows the opposite situation in which effort (e) is known for X.
Causality assignment: As explained earlier, the causal stroke is only assigned to one end of a power bond. This assignment of causal strokes known as *causality assignment* follows the systematic procedure called Sequential Causal Assignment Procedure (SCAP). The SCAP algorithm begins with the elements having the strongest causality constraints and continues until all elements get their causality assigned in the following order: (1) effort and flow sources, (2) I- and C-elements, (3) transformers and gyrators, (4) junctions and (5) R-elements. After that, if a port element has still remained without the causal stroke, it has flexibility in the causality placement, and its causality will be determined at the end [36].
Causal paths: A path between two ports connected via 0-junction, 1-junction, or Transformer (TY) is called a *causal path* if bonds have similar causal stroke directions and the sequence of the causal strokes follows the same pattern. Notice that when a Gyrator (GY) connects two ports the causal stroke direction is altered. Figure 3 shows two different types of causal paths, simple and indirect causal paths, in which direction of causal paths are denoted by green dashed lines.

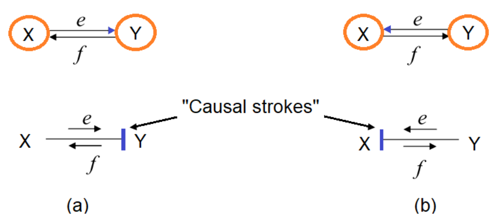


Fig. 2. Causality strokes in bond graphs. (a) Effort is known for Y. (b) Effort is known for X.

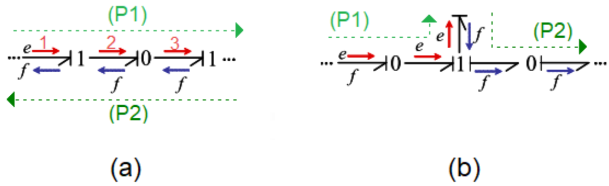


Fig. 3. Causal paths in bond graphs. (a) Simple causal paths and (b) indirect causal paths.

4 Method

In this section, the process of modeling a CPS based on the BG2 model is described. Then the relationships within the cyber and physical layers of a CPS is extracted and relevant metrics of Bond graph and Graph theory are applied to analyze the different characteristics of dependencies within the system.

4.1 BG2 model

As mentioned earlier in section 2, Graph theory has been widely applied to model CPSs in recent years. In these research works, system components are modeled as nodes and the interactions among the nodes are represented by edges. This modeling approach can clearly represent the topology of a system and facilitate analysis of different characteristics of a system based on Graph-based metrics. For instance, the authors in [3] proposed a method to rank the importance of nodes and links in a CPS based on the Closeness Centrality and two novel graph-based metrics, namely the Tacit Input Centrality (TIC) and the Tacit Output Centrality (TOC).

Graph theory provides a high-level and asset-oriented representation of a system which makes it an appropriate choice for modeling the cyber part of CPSs, which relies on information flow to monitor and control the systems, and analyzing the dependency among the IT components. However, studying the dependency in the physical part of a CPS as well as the interactions between the cyber and physical parts requires considering the physics of the system which Graph theory cannot cover. To fill this gap, we can apply Bond graph to model the physical processes of CPSs based on their commodity flows as explained earlier in section 1. Therefore, to study different types of dependencies within a CPS we propose the BG2 model which utilizes Graph theory and Bond graph to model the cyber and physical parts of a CPS respectively and represents the two different types of flow passing through each part, namely commodity flow and information flow. However, unlike the Graph theory, Bond graph demonstrates a system based on the power transfer principle between the system components. Therefore, to be able to apply both Graph theory and Bond graph to model a CPS we leverage the cyber-physical components that exist in CPSs as the interfaces between the cyber and physical parts of the system. Consequently, these interfaces perform as merging points between the Graph and Bond graph diagrams.

A Physical-to-Cyber interface is a component that converts the commodity flow of a CPS into information flow, while a Cyber-to-Physical interface acts the opposite (figure 4). A sensor and an actuator can be seen as the Physical-to-Cyber (P2C) and the Cyber-to-Physical (C2P) interfaces, respectively. As a result, considering the characteristics of cyber and physical parts of a CPS, in our proposed model, the cyber part in which the information flow plays the main role is modeled based on the Graph theory, and the physical part of the system which operates based on the commodity flow is modeled based on the Bond graph, while the P2C and C2P interfaces merge these two parts together. We will explain the BG2 modeling based on a case study represented in section 5 in more detail. Figure 4 illustrates the proposed BG2 modeling for CPSs.

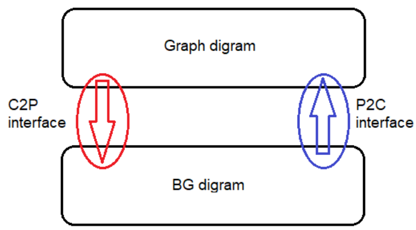


Fig. 4. Conceptual representation of the BG2 model.

4.2 Dependency identification based on the BG2 model

Here, we aim to track dependencies within the system components to study how the behavior of an entity in a CPS depends on the other entities and subsystems. The result of this step provides insight into improving the security of CPSs and to a high extent collaborates in various research domains such as analyzing cascading failures, attack path analysis, and risk management to name a few. For this purpose, after modeling a CPS based on the BG2 model, we utilize the properties of Graph theory and Bond graph to discover dependencies. It is worth mentioning that, *Dependency* is a linkage between two entities in a system, through which the state of one entity influences the state of the other. Besides, the term *Interdependency* defines a bidirectional dependency between two entities in a system in which the state of the first entity affects the state of the second one and vice versa

As explained in subsection 4.1, the cyber part of a CPS is modeled following

Graph theory in the BG2 model. Accordingly, the cyber part can also be portrayed in form of an Adjacency Matrix (A). In Graph theory, an adjacency matrix A is a square matrix used to represent whether the vertex v_i is adjacent to the vertex v_j in a network or not, which shows with one or zero, respectively. Based on the same definition, we define the **Dependency Matrix (D)** which represents the value of information flow (I_{ij}) moves from vertex v_i to vertex v_j in the corresponding cell of the matrix D. Besides, the C2P and P2C interfaces in the BG2 model have interactions with the physical part through the output/input commodity flow. Therefore, to capture the entire interactions for interfaces, an extra column and row labeled as (M) are assigned in the Dependency matrix (D). The pair (M, M) will be further utilized to derive dependencies between the two parts of CPSs as jumping points. Notice that the information flow can be divided into **Sensed data** (I_d) and **Control command** (I_c). This facilitates distinguishing between faults/attacks on monitoring and controlling parts in further steps. The *sensed data* (I_d) is collected from the physical layer by means of P2C interfaces and moves towards the specific components in the cyber layer for monitoring reasons, while the *control command* (I_c) is issued by components like controllers in the cyber layer and moves towards the C2P interfaces to apply the desired changes in the physical process of the system.
Given that the physical part of a CPS is modeled based on Bond graph in the BG2 model, we can extract the dependencies in this part by following the commodity flow and tracking "*Causal Paths*". Causal Paths are one of the significant characteristics of Bond graphs which are derived based on the causality in a system. Indeed, *Causality* indicates the dependencies between the dual variables effort and flow in a system, and specifies the independent variable(s). For all the P2C and C2P interfaces in a BG2 model, we extract pertinent causal paths. These causal paths reveal the dependencies between each interface and system assets in the physical part. Therefore, one can use Dependency matrix D to derive dependencies in the cyber part until reaching an interface (jumping point) and then extract dependencies in the physical part based on the causal paths corresponding to that interface. This enables us to extract higher order of dependencies between those system components that are placed in different parts or subsystems yet affect each other.

For each component in a BG2 model, particularly for the interfaces, we can write a functional dependency relation. Assume that the elements of X, $X = \{x_1, x_2, ..., x_i\}$, are inputs and the elements of Y, $Y = \{y_1, y_2, ..., y_j\}$, are outputs of the component S, so that g expresses a functional input-output relationship ($g : X \rightarrow Y$) as shown in equation 1, which is defined to represent both cyber and physical aspects of this function.

$$Y = g(S|X) \tag{1}$$

Equation 1 represents inputs, outputs, and the device S with the corresponding inner functionality. Consequently, this mathematical representation of the functional properties of a CPS component allows us to analyze both cyber and physical aspects of a relation between inputs and outputs at the same time. This can be further used to identify attack vectors in cyber-physical systems.

5 Case study

In this section, we apply the proposed BG2 model into a realistic cyber physical system shown in figure 5 and extract dependencies within this system based on the method described in subsection 4.2.

5.1 BG2 model of the system

Our case study is developed based on the realistic network infrastructures proposed by Homer et al. [19] and Pan et al. [32], and encompasses four network zones namely Corporate network, Demilitarized zone (DMZ), Field network, and Control network. As shown in figure 5, the physical process of the system occurs in the field network, while the other three networks collaborate in monitoring and controlling. Therefore, the field network in this CPS is considered as the *physical part* and the rest of the network zones form the *cyber part*. To model the cyber part of the case study as a BG2 diagram, the first step is to discover the direction of the interactions within the system components. Homer et al. [19] explained that the web server (A7) and the VPN server (A8) are accessible from the Internet (A6), and the VPN server (A8) has access to the File server (A9), Workstations (A10) and Citrix server (A11). The web server (A7) has only access to the file server (A9). The Citrix server (A11) has access to the Data historian (A3) and Communication servers (A1). Operators can monitor the field network and send commands to the field devices (if necessary) from the Human Machine Interface (HMI). The Communication servers (A1) provide central monitoring and control and additionally interfaced with the data historian (A3) so historical

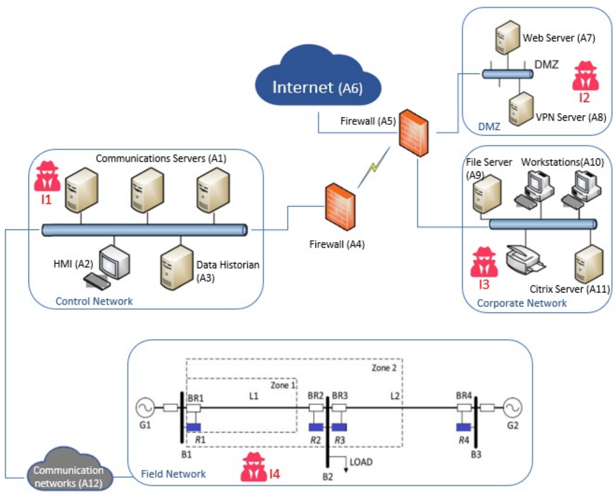


Fig. 5. graphical representation of the case study

data could be collected and preserved and studied outside of real-time operations. Given this information, we model the cyber part of the system as a graph diagram shown in figure 6, in which system components are depicted as nodes (V) and connections among components are represented by links (E). Here, the Graph diagram of the entire system is displayed to help readers compare the graphical representation of a system based on Graph theory and the new proposed BG2 model. In figure 6, devices belonging to the cyber part are depicted in red color, blue circles denoted to those components are placed in the physical part which will be modeled later based on Bond graph, and the P2C/C2P interfaces are depicted in half blue and red.

Following the BG2 model procedures, the second step is to model the *physical part* of the system, i.e. the filed network, based on the Bond graph. In figure 5, the field network is a three-bus two-line transmission system which is a modified version of the IEEE nine-bus three-generator system [32]. This physical part illustrates the process of generating and transmitting power to the consumer (Load). G1 and G2 refer to the power generators, BR1 through BR4 denotes the circuit breakers, and R1 through R4 are relays. Each relay is able to trip and open the related circuit breaker when a fault occurs on a transmission line. Operators are also able to issue commands via HMI to each relay to open and close the corresponding circuit breaker. Based on the port elements of Bond graph represented in figure 1, we model the physical part of the system as shown in the lower part of figure 7. The generators G1 and G2 are modeled as effort sources (Se) and Load L_3 as an R-element. Besides, the dissipation phenomena

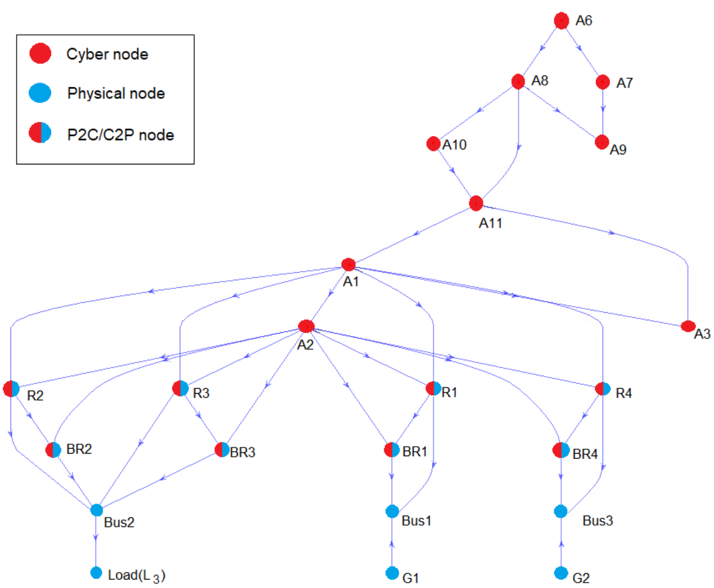


Fig. 6. Digraph of the system

on the transmission lines L1 and L2 are modeled by impedance R:L1 and R:L2, respectively. Following the approach proposed by Umarikar et al. for modeling switches [42], we modeled circuit breakers BR1 through BR4 as 1s-junctions. A circuit breaker switches between two states (on and off) to protect an electrical circuit from damage caused by an over-current or short circuit. Likewise, 1s-junction switches between two states that are determined by Boolean variables U and $\overline{U}$. The role of the Relays in the system is to measure the current that passes through transmission lines and send the trip command to the associated circuit breakers in case of overcurrent. Therefore, as explained in [6], a relay in the BG diagram can be modeled as one sensor which measures the current and one actuator that triggers the corresponding circuit breaker. Considering the roles and input-output of the circuit breakers and relays in the system clears that these components are connecting the cyber and physical parts of the system and are the C2P/P2C Interfaces. In the BG2 model of the system shown in figure 7, cyber components are depicted as solid red nodes while the C2P/P2C Interfaces can be distinguished easily by the red border drawn around port elements.

5.2 Dependency analysis

According to the proposed method explained in section 4.2, dependencies among the components placed in the cyber part of a CPS are represented via the de-

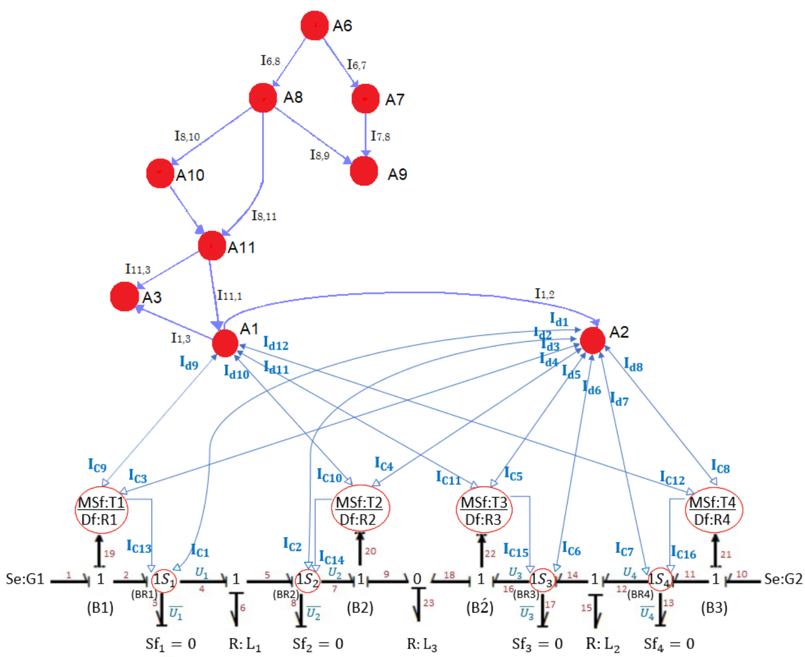


Fig. 7. BG2 representation of the system

pendency matrix D, while dependencies in the physical part derive based on the causal paths. Therefore, considering the BG2 model of the system displayed in figure 7, here, we write the dependency matrix D of the system (see table 1). The next step is to write the causal paths for interfaces. In this regard, we should label the bonds and assign the causal strokes as explained in section 3. Causal strokes display the direction of the effort variable (e) in a BG diagram and are necessary for writing the system equations and causal paths correctly.

Therefore, we assign the causal strokes of effort/flow sources in the first place, then the I- and C-elements, afterward the transformers and gyrators, and finally junctions and R-elements. Following that, as shown in figure 7, all bonds were labeled and the causality assignment was accomplished. After that, we are able to write the causal paths for interfaces that have non-zero values on row M in matrix D. For instance, consider the commodity flow (f_{19}) in table 1 which is an input from the physical part of the system to relay R_1. Based on figure 7, the causal paths terminating at relay R_1 are as follows:

(R1- Path1)$Sf_1 : 0 \xrightarrow{f_3} 1S_1 \xrightarrow{f_2} 1 \xrightarrow{f_{19}} Df : R1$

(R1- Path2) $Sf_2 : 0 \xrightarrow{f_8} 1S_2 \xrightarrow{f_5} 1 \xrightarrow{f_4} 1S_1 \xrightarrow{f_2} 1 \xrightarrow{f_{19}} Df : R1$

(R1- Path3) $Df : R2 \xrightarrow{f_{20}} 1 \xrightarrow{f_7} 1S_2 \xrightarrow{f_5} 1 \xrightarrow{f_4} 1S_1 \xrightarrow{f_2} 1 \xrightarrow{f_{19}} Df : R1$

Notice that for writing the causal paths, we start from Relay R1 and track the sequence of port elements with analogous causality as R1. As an example, in figure 7, relay R1 is connected to effort source $G1$ and $1S_1$-junction. Here, only the direction of casual stroke belonging to the $1S_1$-junction is similar to R1, which means that for extracting the casual path, we have to take a step towards

Table 1. Dependency Matrix D

A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_3	A_1	A_2	R_1	R_2	R_3	R_4	BR_1	BR_2	BR_3	BR_4	M
A_6	0	$I_{6,7}$	$I_{6,8}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A_7	0	0	0	$I_{7,9}$	0	0	0	0	0	0	0	0	0	0	0	0	0
A_8	0	0	0	$I_{8,9}$	$I_{8,10}$	$I_{8,11}$	0	0	0	0	0	0	0	0	0	0	0
A_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A_{10}	0	0	0	0	0	$I_{10,11}$	0	0	0	0	0	0	0	0	0	0	0
A_{11}	0	0	0	0	0	$I_{11,3}$	$I_{11,1}$	0	0	0	0	0	0	0	0	0	0
A_3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A_1	0	0	0	0	0	$I_{1,3}$	0	$I_{1,2}$	I_{C9}	I_{C10}	I_{C11}	I_{C12}	0	0	0	0	0
A_2	0	0	0	0	0	0	0	0	I_{C3}	I_{C4}	I_{C5}	I_{C8}	I_{C1}	I_{C2}	I_{C6}	I_{C7}	0
R_1	0	0	0	0	0	0	I_{d9}	I_{d3}	0	0	0	0	I_{C13}	0	0	0	0
R_2	0	0	0	0	0	0	I_{d10}	I_{d4}	0	0	0	0	0	I_{C14}	0	0	0
R_3	0	0	0	0	0	0	I_{d11}	I_{d5}	0	0	0	0	0	0	I_{C15}	0	0
R_4	0	0	0	0	0	0	I_{d12}	I_{d8}	0	0	0	0	0	0	0	I_{C16}	0
BR_1	0	0	0	0	0	0	0	I_{d1}	0	0	0	0	0	0	0	0	0
BR_2	0	0	0	0	0	0	0	I_{d2}	0	0	0	0	0	0	0	0	0
BR_3	0	0	0	0	0	0	0	I_{d6}	0	0	0	0	0	0	0	0	0
BR_4	0	0	0	0	0	0	0	I_{d7}	0	0	0	0	0	0	0	0	0
M	0	0	0	0	0	0	0	0	f_{19}	f_{20}	f_{22}	f_{21}	f_2	f_5	f_{14}	f_{11}	0

the $1S_1$-junction, not $G1$. Moreover, to write the causal paths for R1 we follow the flow variable (f) as we aim to derive the commodity flow (f_{19}). Following the same approach, one can extract the causal paths for other interfaces.
Based on the above causal paths we have:

$$R1, f_{19} \not\perp\!\!\!\perp \{BR1, BR2, R2\} \tag{2}$$

which implies that R1 and value f_{19} depends on the functionality of BR1, BR2, and R2. As explained in section 4, we can also extract the functional dependency of each system component. Therefore, we can write the functional dependency of components BR1, BR2, and R2 based on equation 1 and considering the pertinent variables shown in dependency matrix D, as follows:

$$U_1 f_4 + \overline{U_1} f_3 = g(BR1|Ic_1, Ic_{13}, f_2) \tag{3}$$

$$U_2 f_7 + \overline{U_2} f_8 = g(BR2|Ic_2, Ic_{14}, f_5) \tag{4}$$

$$U_1 f_4 + \overline{U_1} f_3 = g(BR1|Ic_1, Ic_{13}, f_2) \tag{5}$$

By substituting equations (3-5) into equation 2 we have:

$$R1, f_{19} \not\perp\!\!\!\perp \{Ic_1, Ic_{13}, f_2, Ic_2, Ic_{14}, f_5, Ic_1, Ic_{13}, f_2\}, g(BR1), g(BR2), g(R2) \tag{6}$$

Equation 6 clears that R1 and the value of f_{19} depends on operation of BR1, BR2, and R2 and their inputs $\{Ic_1, Ic_{13}, f_2, Ic_2, Ic_{14}, f_5, Ic_1, Ic_{13}, f_2\}$. Also, based on the matrix D we extract those chains of dependencies in the cyber part that terminates at $R1$ in the following:
$A6 \to A8 \to A11 \to A1 \to R1$,
$A6 \to A8 \to A11 \to A1 \to A2 \to R1$,
$A6 \to A8 \to A10 \to A11 \to A1 \to R1$, and
$A6 \to A8 \to A10 \to A11 \to A1 \to A2 \to R1$.
Therefore, by considering the above dependency chains and equation 6 which are derived based on the causal paths for R1, one can analyze how different components in the case study may affect R1 in case of any accidental failure or cyber-attack. Following this approach not only helps to identify dependencies in a cyber-physical system, but more precisely, it reveals the cause and effect relations between the system components and shed light on studying the behaviors of complex CPSs in different scenarios such as security assessment, failure propagation, or reliability analysis. For instance, the causal path (R1- Path1) reveals the causality between f_{19} and the state of BR1 which is modeled as $1S_1$-junction. Indeed, if $\overline{U_1}$ equals to 1, then this causal path exist and Sf_1 passes through bond 3, i.e $f_3 = Sf_1$. Besides, the causal path (R1- Path1) also shows that the value of f_{19} depends on f_2 and f_3. So, we can see that if $\overline{U_1}$ equals 1, f_{19} will be zero and R1 will sense and send this value to the cyber part. Considering the function of circuit breakers, this $f_{19} = 0$ happens when a fault has occurred on transmission line L1 and BR1 has tripped upon receiving a trip command from R1 or HMI to

protect line L1. In the same way, the causal path (R1- Path2) reveals that f_{19} depends on the functionality and states of $1S_1$-junction (BR1) and $1S_2$-junction (BR2). Here, Sf_2 passes through bond 8 when $\overline{U_2}$ equals to 1. One can write the structural equations for all junctions that exist in the casual path to find the value of f_{19}. Starting from $1S_2$-junction, we have $f_5 = f_8$ if $\overline{U_2}$ is 1 and we know $f_8 = Sf_2$. Notice that in a BG diagram, the same flow passes through all bonds connected to a 1-junction, while a 0-junction implies connected bonds have the same effort. Therefore, when $\overline{U_1}$ equals to 1, because of the 1-junction placed between bonds 4 and 5, we know that $f_5 = f_4$. For the same reason, f_2 is equal to f_{19} and we can conclude that $f_{19} = Sf_2 = 0$. This implies that BR1 is working in a normal situation while BR2 has been tripped because of a fault occurrence on transmission line L1 and the fault was closer to BR2 than BR1. Finally, the last causal path (R1- Path3) reveals the relation between the two relays R1 and R2 as well as commodity flows f_{19} and f_{20}. In this case, if $\overline{U_1} = \overline{U_2} = 1$, then system is in the normal situation and the same flow is passing through transmission line L1, i.e $f_{19} = f_{20}$ and relays R1 and R2 measure the same value. Therefore, based on the above causal paths, we could discover components and states that influence the value of f_{19}. Besides, we showed that these causal paths can reveal different scenarios regarding fault occurrence in a system. Indeed, one of the advantages of Bond graph is its ability to study controllability and observability in a system. Therefore, merging the information gained from the causal paths with the chain of dependencies that can be extracted from the dependency matrix D will assist us to study complex scenarios in which both cyber attacks and faults may occur. For instance, consider the causal path (R1- Path2) as a simple example in which the value of f_{19} depends on the functionality of $1S_1$-junction. Therefore, in the bottom-up direction which relates to the monitoring, any fault, failure, or cyber-attack on $BR1$ can change the value of f_{19} and affect interdependent components in the cyber layer, i.e $\{A1, A2, A11, A10\}$. And from the top-down direction which relates to the controlling feature, any malfunction or cyber attack on $\{A1, A2, A11, A10, R1(Msf : T1)\}$ may change the state of $BR1$ and consequently influence the value of f_{19}.
Based on the matrix D, one can extract dependency chains $A6 \to A8 \to A10 \to A11 \to A1 \to A2$ and $A6 \to A8 \to A11 \to A1 \to A2$ and leverage interfaces BR1-BR4 and R1-R4 to merge dependency chains with pertinent causal paths to evaluate all possible scenarios.
Besides, as explained in section 4, the BG2 model supports all the conventional graph-based metrics. To clear that, we compute the Indegree/Outdegree centrality of the system components based on the Graph diagram depicted in figure 6 and the BG2 model represented in figure 7 as shown in table 2. Comparing the values in table 2 shows a slight difference between the measured values for components placed in the physical part of the system. That is because the BG2 model can provide a realistic abstraction of the physical process of the system and consequently, the Indegree/Outdegree centrality measured based on the BG2 model is more precise than the Graph diagram.

Table 2. Comparing Indegree/Outdegree centrality derive from the BG2 model and Graph diagram.

Nodes:	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_3	A_1	A_2	$G1$	$G2$	$B1$	$R1$	$BR1$	$BR2$	$B2$	$R3$	$B3$	$BR4$	$BR3$	$R2$	$R4$
Out(BG2)	2	1	3	0	1	2	0	6	8	1	1	2	3	2	2	3	3	2	2	2	3	3
In(BG2)	0	1	1	2	1	2	2	5	9	0	0	1	3	3	3	2	3	1	3	3	3	3
Out(Graph)	2	1	3	0	1	2	0	6	8	1	1	0	2	1	1	1	2	0	1	1	2	2
In(Graph)	0	1	1	2	1	2	2	5	9	0	0	3	2	2	2	4	2	3	2	2	2	2

6 Conclusion

In this paper, we proposed the BG2 model to capture and demonstrate the topological and functional characteristics of Cyber Physical Systems as an underlying basis for interdependency analysis. The BG2 model is developed based on Graph theory and Bond Graph to characterize the cyber and physical facets of a CPS and the relationship between them. Interdependency analysis as well as modeling of interdependent systems such as CPSs rely on the understanding of system dynamics and flows. In the BG2 model, the information flow that passes through the cyber components for monitoring and controlling purposes is modeled based on Graph theory, while the Bond graph is applied to model the physical process of the system whose in charge of generating and delivering commodity flow(s). We utilized physical-to-cyber and cyber-to-physical interfaces in the BG2 model to bridge the gap between the data-driven and physics-based driven nature of Graph theory and Bond graph and merge these two underlying methods. In the BG2 model, the relationships between the system components belonging to the cyber part are recorded in a dependency matrix D, causal paths are applied to track the cause and effect relationships between those system components placed in the physical part of a CPS, and the interfaces act as jumping points between these two parts. The interfaces enable us to identify the chains of dependencies for each component, regardless of which part its dependent components belong to or geographical distance. In other words, we can extract the higher order of dependencies for every component in a BG2 model. This facilitates studying cascading failures in CPSs.

In reality, CPSs encounter failures and cyber-attacks. A cyber attack may happen in different parts, and in a worst-case scenario, several attacks may happen together. As explained in section 5, based on the proposed BG2 model, one can distinguish between accidental failures and cyber-attacks in a CPS by analyzing the behavior of the system and dependent components, particularly by noticing the physical process of the system and causal paths. Unlike previous works, BG2 model is not only able to discover the dependencies between the system components but also the cause and effect relationships. Studying the causality in a system can address the "what-if" questions that relate to analyzing changes, that might occur due to a cyber attack or failure, to the system under study. The proposed method also satisfies Graph theory-based metrics that have been applied and developed in previous works. We measured the Indegree/Outdegree centrality based on the Graph diagram and the BG2 model and the comparison

showed that the BG2 model can provide a more realistic result for the physical part of the system.
Interdependency analysis substantially collaborates in improving the security of CPSs and is the foundation of various research domains such as risk propagation, attack path analysis, fault identification and isolation, reliability analysis, and robustness evaluation. Modeling CPSs based on the BG2 model and analyzing dependencies can help us to identify cyber-attacks and predict corresponding consequences and enable us to protect CPSs against them. Furthermore, based on the significant features of Bond Graphs, such as the causal paths, we can derive fault indicator algebraic equations for the physical process of the systems and enhance system controlling and fault isolation. As a result, we aim to apply the BG2 model to develop a new method to discover and analyze cyber-physical attack paths in CPS. It can also help us to investigate the possibility of parallel attack path analysis in cyber-physical systems to identify complex attacks. Designing a unified safety and security risk management method based on the BG2 model is also among our future research plans.

References

1. Abrams, M., Weiss, J.: Malicious control system cyber security attack case study-maroochy water services, australia. Tech. rep., MITRE CORP MCLEAN VA MCLEAN (2008)
2. Addeen, H.H., Xiao, Y., Li, J., Guizani, M.: A survey of cyber-physical attacks and detection methods in smart water distribution systems. IEEE Access **9**, 99905–99921 (2021)
3. Akbarzadeh, A., Katsikas, S.: Identifying critical components in large scale cyber physical systems. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. pp. 230–236 (2020)
4. Akbarzadeh, A., Katsikas, S.: Identifying and analyzing dependencies in and among complex cyber physical systems. Sensors **21**(5), 1685 (2021)
5. Akbarzadeh, A., Katsikas, S.: Dependency-based security risk assessment for cyber-physical systems. Manuscript submitted for publication in International Journal of Information Security (2022)
6. Akbarzadeh, A., Katsikas, S.: Unified it&ot modeling for cybersecurity analysis of cyber-physical systems. IEEE Open Journal of the Industrial Electronics Society (2022)
7. Akbarzadeh, A., Pandey, P., Katsikas, S.: Cyber-physical interdependencies in power plant systems: A review of cyber security risks. In: 2019 IEEE Conference on Information and Communication Technology. pp. 1–6. IEEE (2019)
8. Ashibani, Y., Mahmoud, Q.H.: Cyber physical systems security: Analysis, challenges and solutions. Computers & Security **68**, 81–97 (2017)
9. Benmoussa, S., Bouamama, B.O., Merzouki, R.: Bond graph approach for plant fault detection and isolation: Application to intelligent autonomous vehicle. IEEE Transactions on Automation Science and Engineering **11**(2), 585–593 (2013)
10. Borutzky, W.: Bond graph methodology: development and analysis of multidisciplinary dynamic system models. Springer Science & Business Media (2009)
11. Carhart, N., Rosenberg, G.: A framework for characterising infrastructure interdependencies. International Journal of Complexity in Applied Science and Technology **1**(1), 35–60 (2016)

12. Carreira, P., Amaral, V., Vangheluwe, H.: Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems. Springer Nature (2020)
13. Chen, T.M., Abu-Nimeh, S.: Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
14. Chen, Y., Li, Y., Li, W., Wu, X., Cai, Y., Cao, Y., Rehtanz, C.: Cascading failure analysis of cyber physical power system with multiple interdependency and control threshold. IEEE Access **6**, 39353–39362 (2018)
15. Falahati, B., Fu, Y.: Reliability assessment of smart grids considering indirect cyber-power interdependencies. IEEE Transactions on Smart Grid **5**(4), 1677–1685 (2014)
16. Graja, I., Kallel, S., Guermouche, N., Cheikhrouhou, S., Hadj Kacem, A.: A comprehensive survey on modeling of cyber-physical systems. Concurrency and Computation: Practice and Experience **32**(15), e4850 (2020)
17. Griffor, E.R., Greer, C., Wollman, D.A., Burns, M.J.: Framework for cyber-physical systems: Volume 1, overview. Tech. rep. (2017)
18. Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T., Achiche, S.: Design, modelling, simulation and integration of cyber physical systems: Methods and applications. Computers in Industry **82**, 273–289 (2016)
19. Homer, J., Varikuti, A., Ou, X., McQueen, M.A.: Improving attack graph visualization through data reduction and attack grouping. In: International Workshop on Visualization for Computer Security. pp. 68–79. Springer (2008)
20. House, W.: The national strategy for the physical protection of critical infrastructures and key assets. URL: http://www. whitehouse. gov/pcipb/physical_strategy. pdf (2003)
21. Jensen, J.C., Chang, D.H., Lee, E.A.: A model-based design methodology for cyber-physical systems. In: 2011 7th international wireless communications and mobile computing conference. pp. 1666–1671. IEEE (2011)
22. Khaitan, S.K., McCalley, J.D.: Design techniques and applications of cyberphysical systems: A survey. IEEE Systems Journal **9**(2), 350–365 (2014)
23. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Assessing n-order dependencies between critical infrastructures. International Journal of Critical Infrastructures 6 **9**(1-2), 93–110 (2013)
24. Krotofil, M., Kursawe, K., Gollmann, D.: Securing industrial control systems. In: Security and Privacy Trends in the Industrial Internet of Things, pp. 3–27. Springer (2019)
25. Kumar, P., Merzouki, R., Bouamama, B.O., Koubeissi, A.: Bond graph modeling of a class of system of systems. In: 2015 10th System of Systems Engineering Conference (SoSE). pp. 280–285. IEEE (2015)
26. Li, X., Yu, W.: A hybrid fuzzy petri nets and neural networks framework for modeling critical infrastructure systems. In: 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). pp. 1–6. IEEE (2018)
27. Marashi, K., Sarvestani, S.S.: Towards comprehensive modeling of reliability for smart grids: Requirements and challenges. In: 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering. pp. 105–112. IEEE (2014)
28. Marashi, K., Sarvestani, S.S., Hurson, A.R.: Identification of interdependencies and prediction of fault propagation for cyber–physical systems. Reliability Engineering & System Safety **215**, 107787 (2021)
29. Mathew, J., Ma, L., Tan, A., Weijnen, M., Lee, J.: Engineering asset management and infrastructure sustainability. In: Proceedings of the 5th world congress on engineering asset management (WCEAM 2010). Springer (2011)
30. Merzouki, R., Samantaray, A.K., Pathak, P.M., Bouamama, B.O.: Intelligent mechatronic systems: modeling, control and diagnosis. Springer (2013)

31. Newman, M.: Networks. Oxford university press (2018)
32. Pan, S., Morris, T., Adhikari, U.: Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. IEEE Transactions on Industrial Informatics **11**(3), 650–662 (2015)
33. Rausand, M.: Risk assessment: theory, methods, and applications, vol. 115. John Wiley & Sons (2013)
34. Rinaldi, S.M.: Modeling and simulating critical infrastructures and their interdependencies. In: 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the. pp. 8–pp. IEEE (2004)
35. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine **21**(6), 11–25 (2001)
36. Roychoudhury, I., Daigle, M.J., Biswas, G., Koutsoukos, X.: Efficient simulation of hybrid systems: A hybrid bond graph approach. Simulation **87**(6), 467–498 (2011)
37. Satumtira, G., Dueñas-Osorio, L.: Synthesis of modeling and simulation methods on critical infrastructure interdependencies research. In: Sustainable and resilient critical infrastructure systems, pp. 1–51. Springer (2010)
38. Tagarev, T., Stoianov, N., Sharkov, G.: Integrative approach to understand vulnerabilities and enhance the security of cyber-bio-cognitive-physical systems. In: European Conference on Cyber Warfare and Security. pp. 492–XIX. Academic Conferences International Limited (2019)
39. Tan, R.R., Aviso, K.B., Promentilla, M.A.B., Yu, K.D.S., Santos, J.R.: Input–output models of infrastructure systems. In: Input-Output Models for Sustainable Industrial Systems, pp. 63–74. Springer (2019)
40. Thulasiraman, K., Arumugam, S., Nishizeki, T., Brandstädt, A., et al.: Handbook of Graph Theory, Combinatorial Optimization, and Algorithms. Taylor & Francis (2016)
41. Torres, J.L.S.: Vulnerability, interdependencies and risk analysis of coupled infrastructures: power distribution network and ICT. Ph.D. thesis (2013)
42. Umarikar, A.C., Umanand, L.: Modelling of switching systems in bond graphs using the concept of switched power junctions. Journal of the Franklin Institute **342**(2), 131–147 (2005)
43. Wei, J., Kundur, D.: Biologically inspired hierarchical cyber-physical multi-agent distributed control framework for sustainable smart grids. In: Cyber Physical Systems Approach to Smart Electric Power Grid, pp. 219–259. Springer (2015)
44. White, M.J.: Bond graph modeling of critical infrastructures for cyber-physical security implementation. Master's thesis, Department of Electrical and Computer Engineering, Missouri University of Science and Technology (2021)
45. Wolf, M., Serpanos, D.N.: Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems. Springer (2020)
46. Zhang, Y., Yağan, O.: Modeling and analysis of cascading failures in interdependent cyber-physical systems. In: 2018 IEEE Conference on Decision and Control (CDC). pp. 4731–4738. IEEE (2018)
47. Zhu, W., Milanović, J.V.: Interdepedency modeling of cyber-physical systems using a weighted complex network approach. In: 2017 IEEE Manchester PowerTech. pp. 1–6. IEEE (2017)

ISBN 978-82-326-6576-1 (printed ver.)
ISBN 978-82-326-6986-8 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU

Norwegian University of
Science and Technology