ISSN 0511-5728
The West Indian Journal of Engineering
Vol.45, No.2, January 2023, pp.35-49

The Exigency for Resilient and Cyber-Secure Critical Infrastructure in the Caribbean

Amir Mohammed [a,Ψ], Fasil Muddeen [b], Lincoln Marine [c] and Craig J. Ramlal [d]

Department of Electrical and Computer Engineering, Faculty of Engineering, The University of the West Indies, St Augustine, Trinidad and Tobago, West Indies

[a] Email: amirmohammed45@gmail.com
[b] Email: Fasil.Muddeen@sta.uwi.edu
[c] Email: lincmarine@gmail.com
[d] Email: Craig.Ramlal@sta.uwi.edu

[Ψ] *Corresponding Author*

(Received 23 February 2021; Revised 02 October 2022; Accepted 21 October 2022)

Abstract: *Critical Infrastructures (CIs) are essential assets used to maintain vital societal functions, for example utilities such as power, water, gas, and telecommunication networks. CIs comprise two main parts, namely a: Cyber component and a Physical component, which allow them to operate. Therefore, the occurrence of faults or attacks in either domain can result in the disruption of services, causing negative impacts beyond the system itself. The purpose of this article is to raise awareness within Trinidad and Tobago and, by extension, the Caribbean on the importance of maintaining resilient and cyber secure CIs for the purpose of critical infrastructure protection (CIP) given the current situation. A review of past incidents from 2012 - 2022 taken place both regionally and internationally is discussed, with major emphasis on those occurring in the Caribbean region. These incidents have been presented from the perspective of faults and cyber-attacks affecting CIs resulting in the disruption of services. In responding to frequently occurring scenarios, recommendations on the way forward have been proposed.*

Keywords: *Critical Infrastructures (CIs), Critical Infrastructure Protection (CIP), Resilient Control, Cyber-attacks, Fault Tolerant Control*

Acronyms

CI – Critical Infrastructure
CIP – Critical Infrastructure Protection
CRU – Curacao Refinery Utilities
DoS – Denial of Service
FDI – False Data Injection
IPP – Independent Power Producer
PLC – Programmable Logic Controllers
LAC – Latin America and the Caribbean
PFTCs – Passive Fault Tolerant Control Systems
AFTCs – Active Fault Tolerant Control Systems
HFTCs – Hybrid Fault Tolerant Control Systems
SIDS – Small Island Developing State

1. Introduction

In the last 25 years, several reported faults (Tamronglak et al., 1996) and cyber-attacks have become a source of significant concern internationally and regionally. This has raised the awareness of potential threats and their effects on the critical infrastructures (CIs) within Small Island Developing States (SIDs) locally and regionally. These CIs are more important now than ever due to the COVID-19 pandemic and the increased reliance placed on them. A prime example of major CIs would be the primary health care systems, suddenly being exhausted of their resources. Inherently, CIs consist of both a physical and cyber domain that work together to perform a specific objective. The physical domain can be described as the physical processes implemented for such systems. For example, the energy grid, chemical process equipment, offshore oil and gas platforms. However, these physical processes can be subjected to faults that negatively affect equipment and the overall system objective. The cyber domain can be viewed as the components that do not directly interact with the physical world, such as data computations, monitoring communications, and communication protocols. Similarly, if subjected to cyber-attacks, it disrupts the cyber domain and, in turn, the overall system. Therefore, both domains play an integral part in the daily operations of CIs given the nature of their dependency on each other. This article is divided into three sections. Section 1 highlights the recent disturbances that have manifested themselves within local and regional CI from the perspective of faults and cyber-attacks. Section 2 highlights the concerns surrounding faults and cyber-attacks in the Latin America and Caribbean (LAC) region. Section 3 proposes a way forward based on

https://doi.org/10.47412/DEOX2766

recommendations, and lastly, the research is concluded. To the best of the authors' knowledge, no article has critically reviewed major CI incidents such as these that have taken place locally and in the wider Caribbean, with most cases focused on the English-speaking Caribbean islands and, by extension, countries within Latin America. The article aims to raise awareness for such situations and promote the need for resilient and cyber secure CI in the Caribbean in order to prevent the dangers that these issues present.

2. Recent Disturbances Locally and Regionally

CIs can be defined as complex, large-scale systems that require sophisticated supervisory control systems. These assets are essential for societal functions such as agriculture, water supply, public health, transportation, and electricity generation (Puig et al., 2016). Systems such as these can be subjected to disturbances that may affect their operation daily, resulting in critical situations. A disturbance can be described as a state in which the regular operation of any given system is affected. This article looks at two significant disturbances: 1) faults and 2) cyber-attacks. A fault can be described as the deviation of some specified parameter, whether performance indices or control objective from an acceptable value. Naturally, a fault can then lead to failure when not handled promptly.

In comparison, failure can be described as the system's inability to meet its intended objective under specific conditions. Therefore, failure by definition can be considered more detrimental as compared to a fault. Several faults have occurred locally and within neighboring Caribbean islands, which have resulted in unfavorable situations. These faults have been well studied in literature internationally (Haes Alhelou et al., 2019). Table 1 shows some of the significant power outages around the globe and their associated reported causes.

2.1 Faults Locally and Regionally

Studies have focused on power outages and their associated faults internationally. However, little attention has been placed on documented cases related to the Caribbean region. This section reviews past faults which have resulted in power outages within the LAC region. The following cases have been reported between the years 2013-2022. Over the years, Trinidad has experienced various power outages due to different situations, such as in 2013 (Kowlessar, 2013; Parasram, 2013). The root cause of the problem originated at Phoenix Park Gas Processors Limited which affected gas delivery to power generation units and their dependent sources. Similarly, in 2019, two significant nationwide power outages were recorded across Trinidad. On the 29th of May 2019, the first incident occurred where two power dips were experienced originating from the Desalination Company of Trinidad and Tobago (DESALCOTT) as a result of generator malfunction (Trinidad and Tobago Weather Center, 2019; Doughty, 2019). The second incident occurred in September, which affected Tobago. The issue originated from Cove Eco-Industrial Business Park, causing machines to go offline (Sambrano, 2019; Loop News, 2019). Recently in 2021, various locations across Trinidad were without power due to an issue that originated at one of the power plants (CNC3, 2021; Trinidad and Tobago Guardian, 2021b; TTT News, 2021). A similar situation was experienced in Tobago during maintenance work. A transformer tripped along with the lines from the Milford Bay Substation resulting in a power outage (Trinidad and Tobago Guardian, 2021a).

One of the most recent situations was a 12-hour nationwide power outage which occurred on the 16th of February 2022. The source of the issue was reported as a fault which caused T&TEC's 220 KV lines to trip, causing generation units to go offline (T&TEC, 2022). The water distribution as well as communication network within Trinidad was also impacted negatively. Jamaica has also experienced two severe power outages that took place in 2016. The first occurred on the 17th of April and the second incident took place on the 27th of August which was caused by a fault on the transmission system (Office of Utilities Regulation, 2017). In 2019, the Barbados Light and Power Company sustained power outages due to switch failure in one of the (Spring Garden) substations, while subsequent to that, due to a fault on one of its generating units (Phillips, 2019; BLPC, 2019). Similarly, Belize had several documented cases during 2016 - 2022. In each of these cases, different parts of Belize were reportedly affected by different faults. Areas such as San Pedro town (Belize Electricity Limited, 2016a) and Caye Caulker sustained power outages that lasted up to seven (7) hours (Belize Electricity Limited, 2016b) and in some situations over

Table 1. Significant Power Outages across the world

Country Region	Date	Duration (hours)	Affected People directly/ indirectly (million)	Reported Causes
Brazil	4th Feb 2011	16	53	Transmission line fault and fluctuated power flow
Holland	27thMarch 2015	1.5	1	Plant technical fault
Turkey	31stMarch 2015	4	70	Power System Failure
Ukraine	21st Nov 2015	6	1.2	Power System Failure
US (NY)	1st March 2017	11	21	Cascading failure in transmission system
Sudan	10th Jan 2018	24	41.5	Cascading Failures

Source: Abstracted from Haes Alhelou et al. (2019)

Table 2. A Compilation of Reported Incidents for the LAC Regio**n**

Ref.	Country	Year of Occurrence	Affected Organisation	Reported Causes	Effect of Situation
Trinidad and Tobago Guardian, 2020	Trinidad	July 2020	Methanol Holdings	Pipe Failure	Shut down of Operations
WASA, 2018	Trinidad	February 2018	Point Lisas Desalination Plant	Problem with internal control systems	Affected water supply to residents within Trinidad
Loop News, 2020	Barbados	2020	Barbados Light and Power Company Limited	Fault on the distribution system at the St. Philip substation	Power outage to several areas St Philip, St John St George
Belize Electricity Limited, 2019	Belize	2019	Caye Caulker	Failure of one of the generating units	Loss of Power resulting in load shedding
Belize Electricity Limited, 2022	Belize	2022	Caye Caulker	Failing electronic equipment	Seven (7) power outages
Curacao Chronicle, 2016	Curacao	2016	Curacao Refinery Utilities	Issue with gas turbine at the CRU plant facility	Two successive power outages affecting residents
Curacao Chronicle, 2018	Curacao	2018	Tera Kora substation and Zegu substation	Issue was not identified	Large part of the island was without power for approximately one hour

Table 3. Some Documented Cyber-attacks

Attack Situation	Descriptions of the Events
Siberian Pipeline Explosion (1982)	The first reported cyber security incidents involving a CI was the Siberian Pipeline Explosion which occurred in 1982. The intruder inserted a Trojan horse into the SCADA system.
October (2017)	The Australian Government revealed that hackers compromised an Australian national security contractor in 2016 and stole large amounts of sensitive data.
January (2020)	Mitsubishi announces that a suspected Chinese group had targeted the company as part of a massive cyberattack that compromised personal data of 8,000 individuals as well as information relating to sensitive projects.
May (2020)	Cyber criminals managed to steal $10 million from Norway's state investment fund in a business email.
February (2021)	Ten members of a cybercriminal gang were arrested after a campaign where stole more than $100 million worth of cryptocurrencies.

Sources: Adapted from Sánchez et al. (2019) and CSIS (2021)

the course of three (3) days (Belize Electricity Limited, 2021). Like Belize, Dominica has experienced two island wide power outages in 2015 due to a fault at its Sugar Loaf plant (Anon, 2015).

In 2019, a failure in the regional electrical interconnection system affected Honduras, Nicaragua, Guatemala and El Salvador (The Tico Times Costa Rica News, 2019). There have also been incidents reported in Curacao. The island suffered three successive blackouts (Neaves, 2020). In addition to these previously mentioned events Curacao sustained two power outages in 2019 (Nu.nl, 2020), two in 2020 and another in 2021 (Aquaelectra, 2021). St Lucia has also suffered major power outages. These blackouts experienced on the island occurred during 2019-2021. The island experienced three major island wide power outages as a result of various faults (Joseph, 2019 and 2021; Gaillard, 2020). These scenarios prove to be a concern for daily operations. Table 2 contains additional reviewed incidents, which have not been discussed previously.

2.2 Cyber-attacks Locally and Regionally

Cyber-attacks can be defined as an offensive maneuver that targets computer information systems, computer networks, infrastructures, personal devices, leading to potential loss and harm (Ekici and Altun, 2014). Internationally, Cyber-attacks have become more prevalent and have proven to be of significant concern. Over the years (1982-2021), several cyber-attacks have been documented (see Table 3). The previously mentioned incidents give a brief description of the cyber-attacks performed and the effects on various countries and organisations. It is evident that cyber-attack incidents are escalating and becoming very frequent. This section aims to review cyber-attack incidents for the LAC region for the period 2012-2022 and by extension, raise the level of cyber awareness. In 2012, several eastern Caribbean states were reported as attacked, such as Trinidad and Tobago, Dominican Republic, and Barbados. Trinidad and the Dominican Republic were subject to cyber-attacks which affected their government websites (Bureau of Democracy, 2012). Barbados experienced denial of service attacks affecting Lime Barbados's broadband network customers.

At the end of September 2012, over 1,000 cyber-attacks were reported to the cybercrime investigation and research unit, while 229 websites were reported as attacked, including government, private sector companies and tertiary institutions within Jamaica. Digicel was also subjected to cyber-attacks during 2012-2013. An attacker gained access to the company's database and stole sensitive information. In 2013, Barbados police were reportedly investigating missing data from the oil industry, while in the same period cyber-attacks had

targeted government agencies, financial institutions and private businesses. Within the same year, two Bulgarian nationals reportedly stole over US$ 150,000 from ATMs (Minto-Coy et al., 2018). Cyber-attacks initiated by hackers were also reported affecting various government websites within the Caribbean such as Jamaica (JIS, 2015), St Vincent (CARICOM, 2015) and the Bahamas (BIS, 2015). A similar situation developed in 2019 which affected 11 Trinidad and Tobago government websites, which were breached by Brazilian hackers resulting in these sites being temporarily, disabled (Neaves, 2019).

The government of Bahamas in January 2020, reported a cyber-attack which affected the registrar general's filing information executed by a malicious group (OAGMLA, 2020). The previously mentioned incidents show a trend of emerging and frequent attacks on various countries within the Caribbean. A report released by Microsoft presented data for the period January to March 2017 (OAS, 2018). The data revealed a malware encounter rate which was higher than the global average. Figure 1 shows the encounter rate experienced per country. A similar article (Toapanta et al, 2019) focused on cyber security for the LAC region. The article presented different cases of cybercrimes in Ecuador for 2017, based on location and the types of cyber-attacks, as seen in Figure 2. Essentially, 530 cases were reported where the Pichincha area sustained 145 cases, 24 cases in Manabi, 22 cases in El Oro, 18 cases in Guayas followed by the rest of the Provinces which reported smaller cases which were aggregated.

The popular crimes reported were that of personal, business and government theft. Additionally the cyber-attacks most used and registered in 2018 by banks within the LAC region can be seen in Figure 3. Figure 4 shows the number of web application attacks in the Caribbean in June 2019 based on targeted countries. Puerto Rico recorded the most significant number of attacks followed by Dominican Republic, Bahamas, Jamaica, Haiti, and

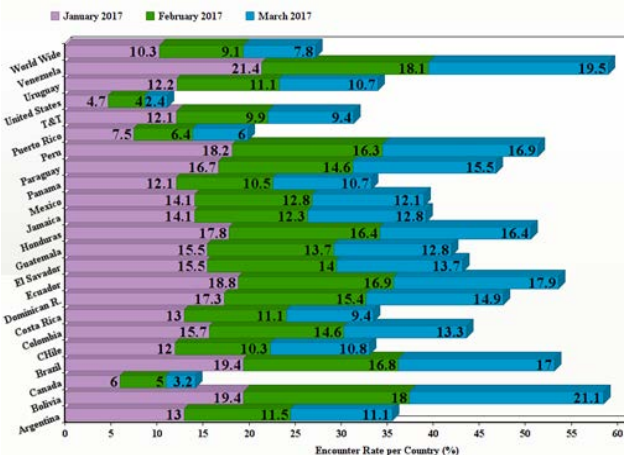

Figure 1. The Encounter Rate Experienced per Country from January to March 2017
Source: Abstracted from OAS (2018)

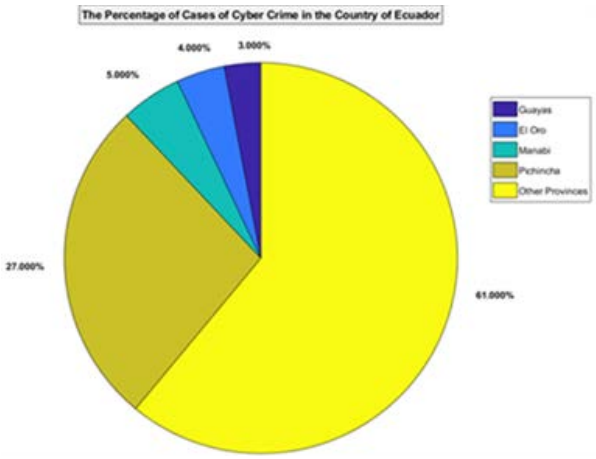

Figure 2. The Percentage of Cases of Cybercrime in the Country of Ecuador in 2017 (Source: Abstracted from Toapanta et al. (2019))

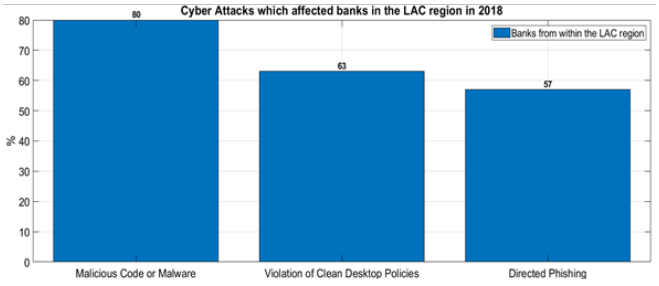

Figure 3. Cyber-attacks Affecting Banks in the LAC Region 2018
Source: Abstracted from Toapanta et al. (2019)

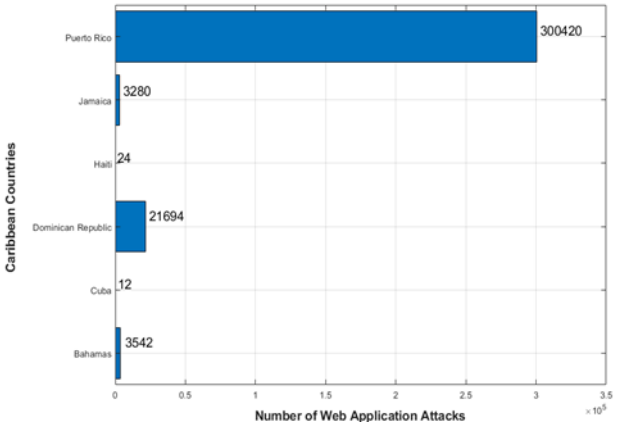

Figure 4. The Number of Web Application Attacks Recorded in June 2019 (Source: Abstracted from Statista (2021))

Cuba. The Caribbean has been highlighted as one of the locations being targeted by ransomware attacks (Hitachi Systems Security, 2020). One prime example of such an incident occurred in late October 2020 that affected one of Trinidad and Tobago's largest conglomerates. A cyber security incident which originated in Barbados migrated to Trinidad, resulting in 17,000 critical files being leaked causing disruptions in its subsidiaries' operations. There was a noticeable increase in advertisements for stolen data

from LAC organisations involving ransomware which increased to 550% from the first quarter of 2020 to the first quarter of 2021 (Caparros, 2021). Figure 5 depicts the websites associated with more than 15 different varieties of ransomware advertising data allegedly stolen from regional organisations.

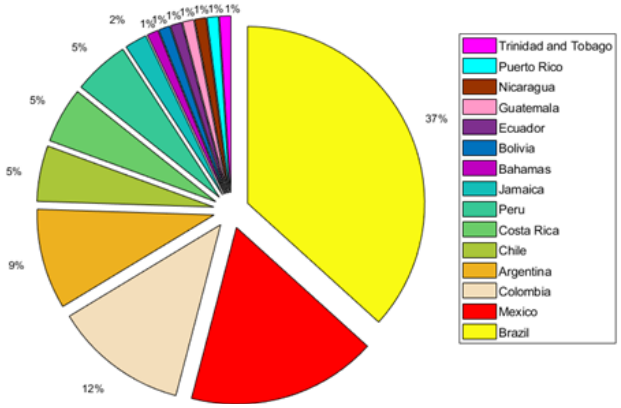

Figure 5. The Percentage of Ransomware Data Theft ADS in LAC by country. Source: Abstracted from Caparros (2021)

The Trinidad and Tobago Cyber Security Incident Response Team published an advisory notice, highlighting that an increase in ransomware attacks targeting Caribbean organisations had been detected (TTCSIRT, 2020). In addition to ransomware, various schemes within the LAC region were reportedly being used to trick individuals and businesses into transferring money known as social engineering attacks (Caparros, 2021). Massy Stores suffered a cyber-attack causing a halt in their business operations of over 21 branches which occurred on the 28th of April 2022 (MST, 2022).

3. Concerns Surrounding Faults and Cyber-attacks in the LAC Region

3.1 Concerns Surrounding Faults

In the previously mentioned incidents reviewed in Section 2, there have been quite a number of power outages which have been caused due to various types of occurring faults. One of the major concerns for such situations, which have become apparent is the aspect of interdependencies. Essentially, this can be thought of as a connection between two or more infrastructures, where the state of one influences the other (Rinaldi et al, 2001). Therefore, in such a situation as it relates to CIs there may exist bi-directional relationships between other CIs and so naturally when one system is affected the dependent sources will experience the effects indirectly due to the nature of the event taking place. Hence, the effects can be felt over large geographic regions and by extension have an impact nationally and globally. It is important to fully understand that there exist various types of interdependencies, such as Physical, Cyber and Geographical and their major differences. Physical interdependency can be considered as where the state of each is dependent on the material output of the other, while cyber interdependency can be defined as where the state and operation of the system is dependent on the information transmitted.

Geographic interdependency can be defined as whereby the local environment can affect changes in all systems within the area (Ouyang, 2014). Identification of such dependencies can be considered a key step into understanding the complex interconnections which may exist between CIs. As a result of such interdependencies, another major issue which has been brought to the forefront is that of power failure. Power failure, based on reported cases highlighted in Section 2, has been widely caused by faults leading to failures within the CI.

Failure of Power systems can be seen as critical as human activities are dependent on power supply, which can be devastating (Haes Alhelou et al., 2019). Such blackouts can lead to social, economic and political impacts which may affect all systems. Therefore, it is evident that the interdependencies, which exist when coupled with the nature of the fault, may produce cascading blackouts. In such a situation the power outage starts as a single system failure and propagates throughout the entire system. It is imperative that faults be handled in a timely manner as if not done the effects can be detrimental.

3.2 Concerns Surrounding Cyber-attacks

The previously mentioned situations highlight the frequency, magnitude and types of cyber-attacks within our region, which is clearly becoming a major concern from the perspective of cost and damage. In 2016, it was reported that the LAC region became a new frontier for cyber-attacks at an estimated cost of $US90 billion per year while, 12% of distributed denial of service attacks (DDoS) were reported as having targeted this region and was on the rise (Jessop, 2016). PricewaterhouseCoopers (PWC) reported that Caribbean firms were not paying enough attention to cybersecurity risks (Curaçao Chronicle, 2017), given the increasing ransomware attacks affecting organisations. In addition to ransomware attacks our region has been plagued with a wide variety of attacks such as Web application, phishing, DoS and even malware attacks. Web application attacks have been mentioned quite frequently in most of the reported cases making it one of the most popular cyber-attacks within our region.

In 2021, the 24th Annual Global CEO Survey for the Caribbean explored the views of 5050 chief executives with Cyber threats listed as one of the top concerns due to high profile cyber-attacks. Figure 6 highlights the areas of concern (PwC, 2021). The Global Cybersecurity Index (GCI) can be used as indicator that measures the commitment of countries to cyber security in order to raise cybersecurity awareness (GCI, 2019). Table 4 compares

the GCIs for 2018 and 2020 for nations within the American Region. The first comparison shows that in 2020 Jamaica's index was calculated as 32.53, which reduced by 8.17 from its 2018 index of 40.7. The table also shows that for every country highlighted, their global associated rank dropped over a two-year period with the exclusion of St Kitts and Guyana.

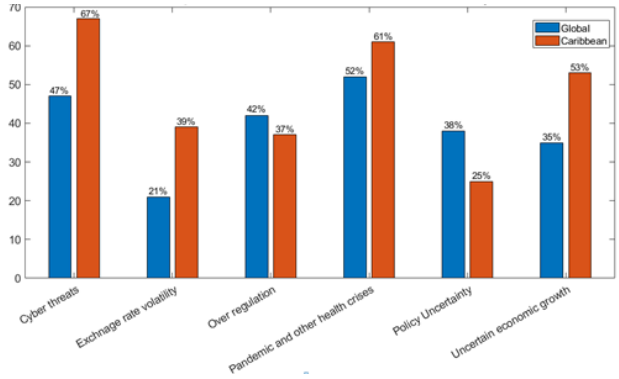

Figure 6. The Top Concerns from the 24th Annual Global CEO Survey conducted in 2021. Source: Based on PwC (2021)

Table 4. Global Cybersecurity Index Comparison for 2018

Country Name	Overall Score	Regional Rank	Global Rank
Jamaica	32.53 (▼8.17)	15 (▼4)	106 (▼12)
Antigua and Barbuda	15.62 (▼9.08)	23 (▼6)	142 (▼29)
Trinidad and Tobago	22.18 (▲3.38)	20 (▼1)	125 (▼2)
Barbados	16.89(▼0.41)	21 (▼1)	139 (▼12)
St. Vincent & the Gren.	12.18 (▼4.72)	28 (▼7)	154 (▼25)
Bahamas	13.37(▼1.33)	24 (▼2)	147 (▼14)
Grenada	9.41 (▼4.89)	31 (▼8)	163 (▼29)
Guyana	28.11 (▲14.9)	17 (▲8)	114 (▲24)
Saint Lucia	10.96 (▲1.36)	29 (0)	158 (▼9)
St Kitts and Nevis	12.44 (▲5.94)	27 (▲3)	153 (▲4)
Dominica	4.2 (▲2.3)	34 (▼1)	174 (▼2)

Sources: Abstracted from GCI (2019 and 2021)

In 2019, a conference on cybercrime strategies for the Caribbean was conducted with the aim of creating a regional response to combating cybercrime by identifying the elements required for an appropriate strategy (CARICOM, 2019). The conference highlighted that most Caribbean countries were at an elementary stage when dealing with cyber-crime. In other cases, there was no cyber-crime legislation established by some participants, while some of the neighboring countries did not provide any data. Table 5 lists the Caribbean nations that contain a national cyber security strategy and the ones currently in the development stages, thus, exposing the region's growing inability to address cyber-attacks. These previously mentioned scenarios highlight the gap that exists as it relates to CIP and the issues which countries within the Caribbean face.

4. Recommendations for the Way Forward

Based on the previously highlighted scenarios and concerns surrounding cyber-attacks and faults, it is imperative CIs be protected from such disturbances. It is clear that the LAC region faces significant adversary activities and so organisations operating in our region should be very weary of this dynamic environment. These incidents, as mentioned earlier (faults/cyber-attacks), especially in the case of cyberattacks, are getting increasingly complex and possibly detrimental due to the level of interconnectedness of the cyber and physical domains. Keeping these concerns in mind, this section proposes recommendations to help alleviate situations in the presence of such disturbances.

It is critical to understand that hackers who in most cases are the initiators of cyber-attacks do not follow any rules or guiding principles, making it a difficult situation to handle. Therefore, the need for having resilient cyber secure CIs is essential for not just CIs but organisations large and small, be it from public or private sector. The owners and operators of CIs and by extension, businesses must understand the potential risks, and ensure that improvements are made to the physical and cyber domains from the aspect of fault tolerance and cyber resilience. In order to attain some level of cyber resilience, the development of a proper defense mechanism is required and so three components must be considered: 1) Prevention, 2) Resilience and 3) Attack Detection and Isolation mechanisms. Prevention mechanisms have been used to alleviate against attacks, starting at an infiltration stage stealing vital information from the system which may be used to perform future attacks. Prevention deals with postponement of the attack (Dibaji et al., 2019). Essentially, prevention mechanisms can be grouped into two categories: 1) Cryptography and 2) Randomisation.

Table 5. Caribbean and Latin America Countries Containing a Cyber-security Strategy and Those in the Developmental Stage

Countries	**Country with a National Cybersecurity Strategy**	**Countries**	**Developing a National Cybersecurity Strategy**
Trinidad and Tobago	Yes (2013)	Guyana	Yes
Dominica Republic	Yes (2018)	Suriname	Yes
Jamaica	Yes (2015)	Ecuador	Yes
Panama	Yes (2013)	Peru	Yes
Costa Rica	Yes (2017)	Belize	Yes
Colombia	Yes (2016)	Barbados	Yes
Guatemala	Yes (2018)		

Source: Abstracted from IDB (2020)

Cryptography is the science of constructing and analysing protocols that prevent third parties from reading private messages (Nadia and Sadkhan, 2020). Cryptographic algorithms make use of the encryption/decryption process of messages.

Encryption is the process of encoding information from sender to receiver ensuring no third party can retrieve the transmitted information. Decryption is the reverse process of encryption which decrypts the information using a secret key that can only be manipulated by the sender/receiver (Laad et al. 2021). The cryptographic system contains the following basic basic components: 1) Plain text, 2) Cipher text, 3) Encryption, 4) Decryption, and lastly 5) Key.

Figure 7 gives a description of the encryption process. There are two types of encryption techniques, symmetric cryptography which is also known as shared secret encryption due to its encryption and decryption keys being the same. The second is known as asymmetric cryptography. In this type of encryption the key is divided into two different keys known as a public and private key. The information is encrypted by the user's public key while it uses its private key to decrypt the information (Arora, 2022). Recent literature (e.g., Hamouda (2020) and Patil et al. (2019)) put forward potential solutions for cryptography. Tables 6 and 7 show the comparison between symmetric and asymmetric algorithms.

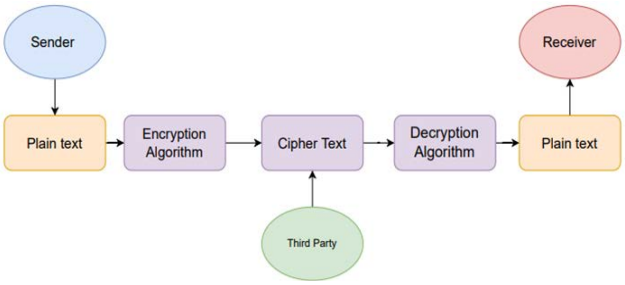

Figure 7. The Encryption/Decryption Process

Randomisation is used as a defensive tool to confuse the potential attacker and has proven useful whenever the predictability of the system may be manipulated by the attackers to obtain key information (Wang et al., 2020). Randomised algorithms have been very useful in a range of mathematical and algorithmic problems also being considered a robust control technique (Dibaji et al, 2019) which has been deployed over the years. Randomisation of data has proven to be successful as it relates to providing confidentiality. There are quite a number of methods which has used randomisation as a means of handling cyber-attacks over the years. These attacks include memory error attacks (Cadar et al, 2008), buffer flow attacks (Fen et al, 2012), attacks from botnets (Al-Jarrah et al, 2015), attacks targeting known static attributes of network devices and systems (Chavez et al, 2015), SQL injection attacks (Perkins et al, 2016), single step and iterative attacks (Xie et al, 2017), code reuse attacks (Yun et al, 2020) and adversarial examples which can affect deep neural networks (Lee et al, 2022).

Resilience can be thought of as a characteristic defined by its ability to withstand and recover from undesirable events (Wei and Ji, 2010). This characteristic may not be inherent and may require integration into the control system design and by extension brings about the topic of Resilient Control Design. Resilient Control is currently being investigated as means by which cyber-attacks can be dealt with (Yuan, Sun and Liu, 2015; Zhao et al., 2022). A resilient control system is one that maintains state awareness and an accepted level of operation normalcy in response to disturbances, including threats of an unexpected behaviour (Rieger, Gertman and McQueen, 2009).

There have been several popular resilience mechanisms which can be used as: 1) Game theoretic approaches, 2) Event triggered control and 3) Trust based approaches are just to name a few. Game theory methods

Table 6. Comparison of Different Symmetric Algorithms

Methods	DES	3DES	AES	IDEA	Blow Fish
Structure of Algorithm	Balanced Feistel	Feistel	Substitution, Permuation	Lai Massey scheme	Feistel
Advantages	Short key	Improved encryption of DES	Larger encryption, faster than 3DES	More secure than AES	Not prone to attacks
Disadvantages	Simple encryption, short key, slow	Slower than DES, susceptible to theoretical attacks	Susceptible to side channel attacks	Frail keys	Considered quicker aside from changing keys

Source: Adopted from Chandra et al. (2014)

Table 7. Comparison of Different Asymmetric Algorithms

Methods	Diffie-Hellman	RSA	DSA	ECC
Structure of Algorithm	Discrete logarithmic	Integer factorisation	Digital Signature	Elliptical curve
Advantages	Short key, fast algorithm	Difficult to decipher private key	Very fast and provides non repudiation and authenticity	Larger key with faster speed, and consumes less power
Disadvantages	Requires short time to decipher key. Susceptible to Man-in-the-Middle Attack	Complexity of key generation	Short lifespan of keys	Higher complexity and increases size of message

Source: Abstracted from Chandra et al. (2014)

focus on strategic interaction between multiple decision makers known as players. The player aims to optimise their objective functions which are dependent on their choices within the game. Game theory allows for a powerful modeling tool which helps describe interactions between players (Mohammed et al., 2022). Game theoretic approaches depend on the structure of the system or based on the type of malicious action which is acting on the cyber layer. The first approach is to model the game tailored for the system under consideration (Sanjab et al, 2017). The second is to model based on the type(s) of the attacks (Dibaji et al., 2019; Miao et al., 2018).

Even triggered control (ETC) has been receiving increased attention for real-time control systems. This type of control allows the control law to be only executed as needed as compared to time-triggered control. Hence, ETC is known for reducing the number of control tasks while maintaining the system's stability. It can be considered reactive and can generate a sensor sampling and control actuation when plant states deviate from a predefined threshold (Heemels et al., 2012). ETC is being used as a method for handling cyberattacks. Based on the frequency of attacks, event-triggered schemes are more appropriate than time-triggered methods for increasing resilience. There are a number of existing event triggered communication mechanisms which can be used to handle cyberattacks such as Denial of Service (DoS), False Data Injection (FDI), and Hybrid attacks. These methods may include communication strategies such as hybrid-triggered (HTS), adaptive event-triggered (AETS), dynamic event-triggered (DETS), memory-based event-triggered (METS), switching-like event triggered (SLETS), and stochastic event-triggered (Wu et al., 2022). Table 8 shows the associated cyberattacks and the event-triggered schemes used for each strategy.

Trust can be viewed as a relationship between two entities where one is considered the evaluator (trustor) and the other is evaluated (trustee). Trust is a relationship established between participating entities facilitated by network activities. The relationship is based on the former interactions and the behaviour exhibited by the participants within the network.

A node may acquire a cumulative value which represents the node's reputation in the given network. Trust modeling helps with the development of functional

Table 8. Cyber Attacks and Associated Communication Strategies

Cyber Attacks	Event Triggered Method	References
DoS	SLETS SETS	(Peng and Sun, 2020) (Peng et al, 2021)
FDI	AETS METS	(Qi et al, 2021) (Wang et al, 2020)
Hyrbid	HTS DETS	Wu et al,2020 Zhang et al 2021

Source: Abstracted from Wu et al. (2022)

parameters that will facilitate aspects such as trustworthiness, user-friendliness and reliability (Muzammal et al., 2020). The aspect of trust should be maintained at three levels: 1) data perception, 2) communication and 3) data fusion (Souissi et al., 2019). There are different trust models which can be used such as the Markov chain model, Arithmetic/Weighting, Directed and Undirected graph-based, Swarm intelligence, Neural Network, Probability based, Fuzzy based, Entropy, Game theory and lastly Bayesian trust model (Shayesteh et al., 2020).

Trust-based approaches have been investigated for scenarios not only limited to cyber-security but also in compromised sub-systems. This approach is comparable to redundancy-based approaches such that, if the numbers of attacks are not significant, then accurate data can be transmitted by trusted nodes within the system (Dibaji et al., 2019). Table 9 highlights some of the methods used for trust based approaches.

Lastly, attack detection and isolation is very important for a proper defense mechanism. It is imperative that these cyber-attacks be detected and located in a timely manner such that the damage sustained to the system can be controlled. Therefore, ensuring CIs have the ability to detect the deviation of its systems states plays a crucial role in maintaining the performance of the CI (Ding et al., 2018). Some of the popular attack detection and isolation strategies may include: 1) Weighted least squares approach (Pei et al., 2021), 2) Quasi Fault Detection and Isolation (Taheri et. al, 2020) and 3) Bayesain detection with binary hypothesis (Han et al., 2021).

For measurement data, a weighted least squares (WLS) approach is one efficient scheme for the defense of attacks. The weighted least squares approach uses a

Table 9. Methods Using Trust-based Approaches for Defending against Cyber Attacks

Techniques	**Attacks Considered**	**Pros and Cons**
Trust based RPL protocol (Airehrour et al, 2018).	Black Hole attack, Selective forward attack.	Evaluation for colluding attacks, energy consumption and E2E delays. Significant packet loss rate, limited mobility of nodes.
Trust for entities is computed using Bayesian Learning and Damper Shaffer Theory for data fusion and computing data trust (Shayesteh et al., 2019).	Malicious Behaviour	Data centric trust management. No consideration for dynamic mobile, and heterogeneous IoT environments
Introduces trust evaluation for secure routing topology construction (Djedjig et al., 2020).	Black hole attack, rank attack.	Efficient in terms of Packet Delivery Ratio, energy consumption, rank changes and throughput. Lack of consideration for mobility factor.

Source: Abstracted from Muzammal et al. (2020)

measurement residual that is usually constructed with the help of WLS observers and then compared to a predetermined threshold to determine the existence of an inaccurate measurement (Ding et al., 2018). This method is considered one of the most popular static state estimation methods which have been used for attack detection. Similar methods that fall under this category include the MF (median filter) and the ML (maximal likelihood) estimation (Du et al., 2022).

There have also been dynamic state estimation methods which have been used to detect the deviation of its systems as seen in the Table 10. Bayesian detection is a traditional detection method as it has been widely applied in data fusion, in sensor networks subjected to cyberattacks (Ding et al., 2018). Statistical anomaly detection models have been becoming increasingly popular in the field of cyber security research.

Some of the popular Bayesian models include: 1) Latent Dirichlet allocation (LDA), 2) Bayesian clustering, and 3) Poisson Factorisation. Bayesian models have the ability to represent uncertainty in a probabilistic manner. Making Bayesian methods attractive for incorporating them in anomaly detection frameworks as the uncertainty can be propagated to predictions resulting in them being more stable. Bayesian models also allow the combination of different types of information in a single framework which allows for a general form for reasoning known as Bayesian reasoning (Perusquía et al., 2022).

Similar to that of cyber resilience, fault occurrence has resulted in mainly power outages from the reviewed cases. The use of Fault Tolerant Control should be incorporated into the design of CIs to help promote the robustness of systems to such disturbances.

There are currently different types of FTC methods. The three main FTC methods are: 1) Passive Fault Tolerant Control (PFTC) methods, 2) Active Fault Tolerant Control (AFTC) methods and 3) Hybrid Fault Tolerant (HFTC) Control methods (Mohammed et al., 2022). In a situation where the nature of any faults occurring is fully known, PFTCs can be utilised, executing the prior defined handling methods which prove to be a major advantage given the control methods use the same conditions in both fault and normal operations. However, this method is susceptible to faults which are not considered and accounted for in the design process and serves as a major disadvantage (Amin and Hasan, 2019). One popular PFTC method is sliding mode control (Merheb, Noura and Bateman, 2013). It provides superior performance compared to other control structures but suffers from an issue known as chattering problem. Other methods which use PFTC include: 1) Linear quadratic control, 2) Fuzzy logic control, 3) Lyapunov based control and even control allocation that have been used in this type of design (Abbaspour et al., 2020).

In a situation where the faults being experienced are unknown and cannot be accurately handled, AFTCs can be used. It uses a fault detection and isolation module along with a reconfiguration law to eliminate the effects of faults. Some popular approaches for AFTCs include: 1) Kalman Filter method (Yuan et al., 2017), 2) Observer based design methods (Wang et al., 2015), 3) Fuzzy Logic method (Liu et al., 2019) and 4) Artificial Neural Networks method (Yin et al., 2016). Table 11 gives a summary of these methods.

Furthermore, HFTCs can be used in situations to combine the effects of PFTCs and that of AFTCs to handle

Table 10. A Comparison between Static and Dynamic Estimation Methods

Category	Methods	Advantages	Disadvantages
Static	WLS MF / ML	Low time complexity Good implementation	Low estimation accuracy Low suitability for large system design
Dynamic	Kalman Filter Extended KF Unscented KF	Good estimation accuracy Applicable to nonlinear models Good Detection rate	High time complexity Easy Divergence

Source: Abstracted from Du et al. (2022)

Table 11. A Comparison of AFTC Methods

FDI Methods	Linear Process	Nonlinear process	Mathematical Modelling	Advantages/ Disadvantages
Kalman Filter	Can be used for linear processes (Typical Kalman Filter)	Can be used for nonlinear processes (Unscented and Extended Kalman Filter)	Model based method which is required for FDI	Considered robust, however considered to be less accurate when compared to other FDI methods. This would result false alarms.
Observer	Can be used for Linear Process	Can be used for nonlinear process Nonlinear unknown input observer)	Model based FDI method for detection and diagnosis	Simple design and considered accurate, however modelling errors and uncertainties can result in slow detection and false alarms.
ANNs	Can be used for linear processes	Can be used for nonlinear processes	Data driven method used for FDI	Considered highly accurate, requires no model for implementation. Requires a large amount of historical data from the system performance.
Fuzzy Logic	Can be used for linear process	Can be used for nonlinear process	Data based method for FDI	Requires no model and so aspects such as disturbances, noise, uncertainties has no effect on the method. However, requires some expert knowledge of the system for implementation of rule base.

Sources: Abstracted from Mohammed et al. (2022) and Thirumarimurugan et al. (2016)

both situations simultaneously (Amin and Hasan, 2019). HFTC operates on the basis of using a passive controller which can be exploited for safe and reliable control until a reliable controller is acquired based on the information generated by the FDI unit. Naturally, the controller has more time to attain information from the fault and so a reconfigured law can take effect (Tahri et al., 2018; Alsuwian et al., 2022).

Adopting the previously mentioned FTC methods and the cyber resilience methods, allow CIs to handle a wide range of disturbances from the cyber and physical domain and by extension promotes CIP. In addition to these methods, there have been a number of best practices which can be used as a guide for CIP as suggested in (OAS, 2018). These practices include:

1) Identifying the clear division of responsibilities which involves government leadership in accordance with multiple stakeholders working together to develop a CIP strategy.
2) Creating a holistic approach using viewpoints from all sectors as the operation of CIs involves several entities such as public private sectors and academia.
3) Development of frameworks guidelines and procedures coordinated by the government with emphasis being placed on risk management.
4) Set a Security baseline which helps in managing cybersecurity risks.
5) Supporting dynamic solutions which are able to rival the ever changing cyber environment.
6) Fostering Trust between public private partnerships which facilitates the exchange of information in an open manner.
7) Development of early warning mechanisms which minimises the impact of cyber-attacks.
8) Investing into in human and technical resources such as cybersecurity as CIP requires experts from several fields of study. Therefore, this may require tertiary level institutions to offer extensive programmes within this field.
9) Improve cyber resilience, and
10) Participate in an international network.

These practices have been advocated in literature (Brunner and Suter, 2008; OAS, 2009; CIIP, 2015; Luiijf et al., 2016; Garcia and Jeun, 2016; Barrett, 2018; Cheng et al., 2021) and can be used to give insight to CIP strategies.

By application of these practices, CI organisations could foster a suitable defensive system. The disseminated knowledge of responsibilities and the concurring consequences would give a clear indication of the importance of fulfilling one's roles and thus serve as a means in which incorrigible practices could be prevented. The government's role by extension plays a bigger part in CIP being one of the bodies which are required to coordinate partnerships among sectors, both private and international, as well as update and disseminate information. Finally, the development of a continuously improved cybersecurity framework which serves as the main shield against cyber attacks at all stages from early detection and warning to prevention and isolation/handling is essential.

Fostering competent personnel, forming industrial partnerships and developing cutting-edge technology are each equally costly. That with the addition of trust may prove to be even more difficult as there is a reluctance of companies to divulge trade secrets as well as exposing potential vulnerabilities that may exist within their infrastructure, as situations like these can be used in the context of experience gained to help better prepare for similar future events. There is a need to prioritise the aforementioned practices. One of the most important aspects is investing into human and technical resources to foster an intrinsic CIP workforce. Table 12 provides some training solutions for Cyber Security and CIP.

It is also one of the options in which the benefit is directly obtained by the investing CI organisations. By achieving practice (8), this paves the way for developing a self-sustaining cybersecurity system since practices (4), (7) and (9) would be achievable based on the level of investment placed on training. The issue of trust varies based on the organisations involved, and further highlights the importance of the governing body that will be required to coordinate and manage partnerships to help foster the aspect of trust amongst participating entities. These partnerships will prove to be extremely useful from all aspects. The remaining practices involve government participation which will ensure CIP.

5. Conclusion

In this article, a detailed review of previous incidents that have taken place in the form of faults and cyber-attacks over the years has been conducted. The Caribbean region

Table 12. Description of training solutions for Cyber Security and CIP

Work	Proposed Solutions	Descriptions
(Willems et al, 2011)	Tele lab: system for hands on IT security training in a remote virtual lab environment	Structured virtual training followed by detailed practical exercises
(Tang et al, 2017)	Interactive cyber security defense training inspired by web based learning theory	Training attack and defense via a multitude of databases for facilitating vulnerability and exploitation.
(Proctor, 2016)	CS awareness Training Programme Efficacy Evaluation	Awareness of need, stratification and possible future of CS measures.
(Beuran et al, 2018)	CyTrONE: integrated cybersecurity training framework	Individual tailored training of attack, defense and forensic analysis of CS development in dynamic training environments.

Sources: Abstracted from Chowdhury and Gkioulos (2021

is under attack and faces a difficult task related to CIP. Necessary measures such as policies and strategies must be put in place to help combat these incidents and mitigate the effects of such occurrences. Entities such as CI owners/operators and, by extension, businesses must see the need to maintain resilient cyber secure organisations given the ever-changing environment to ensure that daily operations are not affected. Resilient control and Fault tolerant control can be used as two critical methods to reduce the effects of such scenarios in accordance with the general guidelines proposed for CIP. Future work includes a second article which reviews and analyses the theory of fault tolerant and resilient cyber secure methods that will help protect CIs from adverse situations.

References:

Abbaspour, A., Mokhtari, S., Sargolzaei, A. and Yen, K.K. (2020), "A survey on active fault-tolerant control systems", *Electronics*, Vol.9, No.9, pp.1513.

Airehrour, D., Gutierrez, J., and Ray, S.K. (2018), "A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol", *Journal of Telecommunications and the Digital Economy*, Vol.6, No.1, pp.41-49.

Al-Jarrah, O.Y., Alhussein, O., Yoo, P.D., Muhaidat, S., Taha, K., and Kim, K. (2015), "Data randomisation and cluster-based partitioning for botnet intrusion detection", *IEEE Transactions on Cybernetics*, Vol.46, No.8, pp.1796-1806.

Alsuwian, T., Tayyeb, M., Amin, A.A., Qadir, M.B., Almasabi, S., and Jalalah, M. (2022), "Design of a hybrid fault-tolerant control system for air-fuel ratio control of internal combustion engines using genetic algorithm and higher-order sliding mode control", *Energies*, Vol.15, No.15, pp.5666.

Amin, A.A. and Hasan, K.M. (2019), "A review of fault tolerant control systems: Advancements and applications", *Measurement*, Vol.143, pp.58-68.

Anon, (2015), "DOMLEC explains recent power outages", *Dominica Vibes News*, [online] Available at: https://www.dominicavibes.dm/news-167265/ [Accessed 18 Oct. 2021].

Aquaelectra (2021), "Root cause analysis Blackout events", [online] Aquaelectra. Available at: https://www.aqualectra.com/technical-reports/ [Accessed 21 Feb. 2022].

Arora, S. (2022), "A review on various methods of cryptography for cyber security", *Journal of Algebraic Statistics*, Vol.13, No.3, pp.5016-5024.

Barrett, M.P. (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. NIST Cybersecurity Framework, [online] doi:http://dx.doi.org/10.1002/https://dx.doi.org/10.6028/NIST.CSWP.04162018.

Belize Electricity Limited (2016a), "BEL Apologises to Customers in San Pedro Town for Extensive Power Interruption", [online] Available at: https://www.bel.com.bz/press_releases/2016/July/07072016.pdf [Accessed 1 Feb. 2022].

Belize Electricity Limited (2016b), "BEL Locates Fault Responsible for San Pedro Power Interruption", [online] Belize Electricity Limited. Available at: https://www.bel.com.bz/press_releases/2016/November/11032016.pdf [Accessed 22 Feb. 2022].

Belize Electricity Limited (2019), "BEL Addresses Generation Issues on Caye Caulker", [online] Belize Electricity Limited. Available at: https://www.bel.com.bz/press_releases/2019/BEL%20Addresses%20Generation%20Issues%20on%20Caye%20Caulker.pdf [Accessed 1 Feb. 2022].

Belize Electricity Limited (2021), "BEL Provides Update on Unplanned Outage in the Belize District", [online] Belize Electricity Limited. Available at: https://www.bel.com.bz/press_releases/2021/BEL%20Provides%20Update%20on%20Unplanned%20Outage%20in%20the%20Belize%20District.pdf [Accessed 2 Feb. 2022].

Belize Electricity Limited (2022), "BEL Working to Resolve Generation Issues on Caye Caulker", [online] Belize Electricity Limited. Available at: https://www.bel.com.bz/press_releases/2022/BEL%20Working%20to%20Resolve%20Generation%20Issues%20on%20Caye%20Caulker.pdf [Accessed 17 Feb. 2022].

Beuran, R., Tang, D., Pham, C., Chinen, K.I., Tan, Y., and Shinoda, Y. (2018), "Integrated framework for hands-on cybersecurity training: CyTrONE", *Computers and Security*, Vol.78, pp.43-59.

BIS (2015), "Several Bahamas' government websites hacked by Tunisian Islamist activist group", *The Bahamas Weekly*, [online] Bahamas Information Services, Available at: http://www.thebahamasweekly.com/publish/bis-news-updates/Several_Bahamas_government_websites_hacked_by_Tunisian_Islamist_activist_group_printer.shtml [Accessed 22 Feb. 2022].

BLPC (2019), "Statement from the Managing Director of BLPC" The Barbados Light and Power Company Limited, [online] The Barbados Light and Power Company Limited. Available at: https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A3431794906857998%7D&path=%2Fnotes%2Fnote%2F&_rdr [Accessed 22 Feb. 2022].

Brunner, E.M. and Suter, M. (2008), "An inventory of 25 national and 7 international critical information infrastructure protection policies", *International CIIP Handbook 2008/2009*, ETHZurich: Center for Security Studies.

Bureau of Democracy, Human Rights and Labor (2012), "2011 Country Reports on Human Rights Practices - Dominican Republic", [online] refworld. Available at: https://www.refworld.org/docid/4fc75aa473.html [Accessed 12 Sep. 2021].

Cadar, C., Akritidis, P., Costa, M., Martin, J.P., and Castro, M. (2008), "Data randomisation", *Technical Report TR-2008-120*, Microsoft Research, p. 115.

Caparros, Juan C.G. (2021), "Top Cyber Threats to Latin America and the Caribbean", *Mandiant.* Available at: https://www.mandiant.com/resources/blog/top-cyber-threats-to-latin-america-and-the-caribbean (Accessed: 22 Feb 2021).

CARICOM (2015), "St Lucia tightens cyber security after hacking of SVG site", [online] Available at: https://caricom.org/st-lucia-tightens-cyber-security-after-hacking-of-svg-site/ [Accessed 15 Dec. 2021].

CARICOM (2019), "Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community", [online] Available at: https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c [Accessed 1 Dec. 2021].

Chandra, S., Paira, S., Alam, S.S., and Sanyal, G. (2014), "A comparative survey of symmetric and asymmetric key cryptography", *Proceedings of the 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, IEEE, November, pp. 83-93.

Chavez, A.R., Stout, W.M., and Peisert, S. (2015), "Techniques for the dynamic randomisation of network attributes", *Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST)*, IEEE, September, pp. 1-6

Cheng, L., Liu, Y., and Zhao, Y. (2021), "Exploring the US institutional discourse about critical information infrastructure protection (CIIP): A corpus-based analysis", *International Journal of Legal Discourse*, Vol.6, No.2, pp.323-347.

Chowdhury, N. and Gkioulos, V. (2021), "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review*, Vol.40, pp.100361.

CIIP (2015), "Critical Information Infrastructures Protection (CIIP) approaches in EU", [online] Available at: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf.

CNC3 (2021), "T&TEC: Power outages due to problems at power plant", *CNC3*, [online] 22 Dec. Available at: https://www.cnc3.co.tt/ttec-power-outages-due-to-problems-at-power-plant/ [Accessed 21 Nov. 2021].

CSIS (2021), "Significant Cyber Incidents", Center for Strategic and International Studies, [online] www.csis.org. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. [Accessed 21 Dec. 2021]

Curaçao Chronicle (2016), "Problems at CRU: several areas without power", [online] Available at: https://curacaochronicle.com/local/problems-at-cru-several-areas-without-power/ [Accessed 7 Feb. 2022].

Curaçao Chronicle (2017), "Analyst says Caribbean companies at risk for ransomware attacks", [online] Available at: http://curacaochronicle.com/tech/analyst-says-caribbean-companies-at-risk-for-ransomware-attacks/ [Accessed 15 Oct. 2021].

Curaçao Chronicle (2018), "Power failure affects large area of the island", [online] Available at: https://curacaochronicle.com/local/power-failure-affects-large-area-of-the-island/ [Accessed 18 Oct. 2021].

Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., and Chakrabortty, A. (2019), "A systems and control perspective of CPS security", *Annual Reviews in Control*, Vol.47, pp.394-411.

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., and Zhang, X.-M. (2018), "A survey on security control and attack detection for industrial cyber-physical systems", *Neurocomputing*, Vol.275, pp.1674-1683.

Djedjig, N., Tandjaoui, D., Medjek, F., and Romdhani, I. (2020), "Trust-aware and cooperative routing protocol for IoT security", *Journal of Information Security and Applications*, Vol.52, pp.102467.

Doughty, M. (2019), "Electrical fault results in power dip", *Trinidad and Tobago Newsday*, [online] 30 May. Available at: https://newsday.co.tt/2019/05/30/electrical-fault-results-in-power-dip/ [Accessed 20 Dec. 2021].

Du, D., Zhu, M., Li, X., Fei, M., Bu, S., Wu, L., and Li, K. (2022), "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems", *Journal of Modern Power Systems and Clean Energy*, pp.1-18, available at: https://ieeexplore.ieee.org/document/9837836

Ekici, R. and Altun, H.R. (2014), "Network-Centric Operations, Vulnerabilities to Cyber-attacks", The Clute Institute.

Fen, Y., Fuchao, Y., Xiaobing, S., Xinchun, Y., and Bing, M. (2012), "A new data randomisation method to defend buffer overflow attacks", *Physics Procedia*, Vol.24, pp.1757-1764.

Gaillard, S. (2020), "St Lucia experiences island-wide power outage", [online] Loop. Available at: https://stlucia.loopnews.com/content/st-lucia-experiences-island-wide-power-outage [Accessed 5 Oct. 2021].

García Zaballos, A. and Jeun, I. (2016), "Best practices for critical information infrastructure protection (CIIP): Experiences from Latin America and the Caribbean and selected countries", available at: https://publications.iadb.org/en/best-practices-critical-information-infrastructure-protection-ciip-experiences-latin-america-and.

GCI (2019), "GCI 2018", Global Security Index, [online] Switzerland, Geneva: ITU Publications, pp.56–57, Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [Accessed 22 Feb. 2022].

GCI (2021), "GCI 2020", Global Cybersecurity Index [online] Switzerland, Geneva: ITU Publications, pp.28–29. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf [Accessed 22 Feb. 2022].

Haes Alhelou, H., Hamedani-Golshan, M., Njenda, T., and Siano, P. (2019), "A survey on power system blackout and cascading events: Research motivations and challenges", *Energies*, Vol.12, No.4, pp.682.

Hamouda, B.E.H.H. (2020), "Comparative study of different cryptographic algorithms", *Journal of Information Security*, Vol.11, No.3, pp.138-148.

Han, K., Duan, Y., Jin, R., Ma, Z., Wang, H., Wu, W., Wang, B., and Cai, X. (2021), "Attack detection method based on bayesian hypothesis testing principle in CPS", *Procedia Computer Science*, Vol.187, pp.474-480.

Heemels, W.P., Johansson, K.H., and Tabuada, P. (2012), "An introduction to event-triggered and self-triggered control", *Proceedings of the 2012 IEEE 51st Conference on Decision and Control (CDC)*, IEEE, December, pp. 3270-3285

Hitachi Systems Security (2020), "The Caribbean: A Ransomware Target?" [online] November, Available at: https://hitachi-systems-security.com/the-caribbean-a-ransomware-target/ [Accessed 21 Feb. 2022].

IDB (2020), "2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean", [online] Inter American Development Bank (IDB), Available at: https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean [Accessed 22 Feb. 2022].

Jessop, D. (2016), "Action needed to address Caribbean cyber security", [online] The Caribbean Council, Available at: https://caribbean-council.org/wp-content/uploads/2016/10/The-View-From-Europe-Oct-31-Action-needed-to-address-cyber-security.pdf [Accessed 22 Feb. 2022].

JIS (2015), "Police Investigating Hacking of JIS Website", Jamaica Information Service, [online] 25 Jun. Available at: https://jis.gov.jm/police-investigating-hacking-of-jis-website/ [Accessed 22 Feb. 2022].

Joseph, C. (2019), "Internal Fault Triggers System Shutdown", [online] LUCELEC. Available at: https://www.lucelec.com/content/internal-fault-triggers-system-shutdown?fbclid=IwAR2aPUL_qB92XcPgKEirZ8h40Fh9CFPPyEHfi_flc935St_53RxrX-jMTd4 [Accessed 12 Sep. 2021].

Joseph, C. (2021), "Statement on Second Island Outage", Friday, September 10, 2021. [online] LUCELEC. Available at: https://www.lucelec.com/tags/power-outage#:~:text=Castries%2C%20May%2026%2C%202015%20%E2%80%93 [Accessed 2 Dec. 2021].

Kowlessar, G. (2013), "Three major blackouts in three years", [online] Available at: https://www.guardian.co.tt/article-6.2.398271.6a3bd01827 [Accessed 7 Feb. 2022].

Laad, A. and Sawant, K. (2021), "A literature review of various techniques to perform encryption and decryption of data", *Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, IEEE, June, pp. 696-699

Lee, S., Kim, H., and Lee, J. (2022), "Graddiv: Adversarial robustness of randomised neural networks via gradient diversity regularisation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, available at: https://ieeexplore.ieee.org/abstract/document/9761760

Liu, X., Zhai, D., Li, T., and Zhang, Q. (2019), "Fuzzy-approximation adaptive fault-tolerant control for nonlinear pure-feedback systems with unknown control directions and sensor failures", *Fuzzy Sets and Systems*, Vol.356, pp.28-43.

Loop News (2019), "Tobago suffers island-wide blackout", Loop Trinidad and Tobago, [online] Available at:

https://tt.loopnews.com/content/tobago-suffers-island-wide-blackout [Accessed 22 Feb. 2022].

Loop News. (2020), "Equipment failure causes New Year's Day power outage", *Loop Barbados*, [online] Available at: https://barbados.loopnews.com/content/equipment-failure-causes-new-year-power-outage [Accessed 18 Oct. 2021].

Luiijf, H.A.M., van Schie, T.C.C., van Ruijven, T.W.J., and Huistra, A.W.W. (2016), The GFCE-MERIDIAN good practice guide on critical information infrastructure protection for governmental policy-makers, available at: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

Merheb, A.R., Noura, H., and Bateman, F. (2013), "Passive fault tolerant control of quadrotor uav using regular and cascaded sliding mode control", *Proceedings of the 2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, IEEE, October, pp. 330-335

Miao, F., Zhu, Q., Pajic, M., and Pappas, G.J. (2018), "A hybrid stochastic game for secure control of cyber-physical systems", *Automatica*, Vol.93, pp.55-63.

Minto-Coy, I.D. and Henlin, M.G.G. (2018), "The development of cybersecurity policy and legislative landscape in Latin America and Caribbean States", *Cyber Security and Threats*, pp.286-308.

Mohammed, A., Muddeen, F., Ramlal, C.J., and Marine, L. (2022), "A comprehensive review of fault tolerant and resilient cyber-secure strategies for critical infrastructure protection", *Industrial Engineering and Management Journal*, Vol.1, No.1, June/July, pp.66-76

MST (2022), "Media Release: Cyber Attack Identified as Cause of Technical Shutdown" Massy Stores Trinidad, [online] Available at: https://massystorestt.com/media-release-cyber-attack-identified-as-cause-of-technical-shutdown/, [Accessed 1 May 2022]

Muzammal, S.M., Murugesan, R.K., and Jhanjhi, N.Z. (2020), "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches", *IEEE Internet of Things Journal*, Vol.8, No.6, pp.4186-4210.

Nadia, A.W. and Sadkhan, S.B. (2020), "Cryptography techniques within SCADA system: A survey", *Proceedings of the 2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, IEEE, September, pp. 89-94

Neaves, J. (2019), "Hack Attack" *Trinidad and Tobago Newsday*. [online] Available at: https://newsday.co.tt/2019/07/27/hack-attack/ [Accessed 22 Feb. 2022].

Neaves, J. (2020), "Curaçao suffers three blackouts in one week", Loop, [online] 14 Dec. Available at: https://caribbean.loopnews.com/content/curacao-suffers-three-blackouts-one-week [Accessed 5 Nov. 2021].

Nu.nl (2020), "Curaçao has been hit by an unprecedented series of power outages this week", [online] Nu.nl. Available at: https://www.nu.nl/buitenland/6096402/curacao-al-urenlang-zonder-stroom-vierde-stroomstoring-in-week-tijd.html?redirect=1 [Accessed 12 Nov. 2021].

OAGMLA (2020), "OAG Press Statement - Hack of RGD Database", [online] Office of the Attorney-General & Ministry of Legal Affairs, The Government of the Bahamas, Available at: https://www.bahamas.gov.bs/wps/portal/public/gov/government/news/oag%20press%20statement%20-%20hack%20of%20rgd%20database/ [Accessed 12 Jul. 2021].

OAS (2009). OAS - Organisation of American States: Democracy for peace, security, and development, [online] Available at: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf.

OAS (2018), "Democracy for peace, security, and development", [online] OAS - Organisation of American States. Available at: https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-009/18 [Accessed 20 Dec. 2020].

Office of Utilities Regulation (2017), "2016 Outage Report - investigation on Electricity System Total Shutdown", August 27 [online] Available at: https://our.org.jm/document/jps-submits-2017-annual-tariff-adjustment-proposal-2/ [Accessed 15 Dec. 2021].

Ouyang, M. (2014), "Review on modeling and simulation of interdependent critical infrastructure systems", *Reliability Engineering and System Safety*, Vol.121, pp.43-60.

Parasram, J. (2013), "Jyoti Communication: T&T national blackout caused by malfunction in gas supply system", [online] Jyoti Communication, Available at: http://jyoticommunication.blogspot.com/2013/03/t-national-blackout-caused-by.html [Accessed 15 Dec. 2021]

Patil, A., Banerjee, S., and Borkar, G. (2019), "A survey on securing smart gadgets using lightweight cryptography", *Lecture Notes on Data Engineering and Communications Technologies*, pp.503-515

Pei, C., Xiao, Y., Liang, W., and Han, X. (2021), "A deviation-based detection method against false data injection attacks in smart grid", *IEEE Access*, Vol.9, pp.15499-15509.

Peng, C. and Sun, H. (2020), "Switching-like event-triggered control for networked control systems under malicious denial of service attacks", *IEEE Transactions on Automatic Control*, Vol.65, No.9, pp.3943-3949.

Peng, C., Wu, J., and Tian, E. (2021), "Stochastic event-triggered H ∞ control for networked systems under denial of service attacks", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol.52, pp.4200-4210

Perkins, J., Eikenberry, J., Coglio, A., Willenson, D., Sidiroglou-Douskos, S., and Rinard, M. (2016), "AutoRand: Automatic keyword randomisation to prevent injection attacks", *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, Cham, July, pp.37-57

Perusquía, J.A., Griffin, J.E., and Villa, C. (2022), "Bayesian models applied to cyber security anomaly detection problems", *International Statistical Review*, Vol.90, No.1, pp.78-99.

Phillips, L.D. (2019), "Fuel issues blamed for power outages in Barbados", *Loop News*, [online] 19 Nov. Available at: https://tt.loopnews.com/content/fuel-issues-blamed-power-outages-barbados [Accessed 10 Nov. 2021].

Proctor, W.R. (2016), *Investigating the Efficacy of Cybersecurity Awareness Training Programs*, Doctoral dissertation, Utica College

Puig, V., Escobet, T., Sarrate, R., and Quevedo, J. (2016), "Fault detection and isolation in critical infrastructure systems", *Critical Information Infrastructures Security*, pp.3-12.

PwC (2021), "A leadership agenda to take on tomorrow 24th Annual Global CEO Survey - Caribbean findings", [online] PriceWaterhouseCoopers, Available at: https://www.pwc.com/cb/en/pwc-ceo-survey.html [Accessed 22 Feb. 2022].

Qi, Y., Yuan, S., and Niu, B. (2021), "Asynchronous control for switched TS fuzzy systems subject to data injection attacks via adaptive event-triggering schemes", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 52, pp.4658-4670

Rieger, C.G., Gertman, D.I., and McQueen, M.A. (2009), "Resilient control systems: Next generation design research", *Proceedings of the 2nd Conference on Human System Interactions 2009*, IEEE. May, pp. 632-636

Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K. (2001), "Identifying, understanding, and analysing critical infrastructure interdependencies", *IEEE Control Systems Magazine*, Vol.21, No.6, pp.11-25.

Sambrano, C. (2019), "T&TEC committee to probe Tobago

blackout", *Trinidad and Tobago Guardian*, [online] 29 Sep. Available at: https://www.guardian.co.tt/news/ttec-committee-to-probe-tobago-blackout-6.2.948331.26c85b58f5 [Accessed 22 Feb. 2022].

Sánchez, H.S., Rotondo, D., Escobet, T., Puig, V., and Quevedo, J. (2019), "Bibliographical review on cyber-attacks from a control oriented perspective", *Annual Reviews in Control*, [online] Vol.48, pp.103–128. Available at: https://www.sciencedirect.com/science/article/pii/S1367578819300288 [Accessed 28 Feb. 2020].

Sanjab, A., Saad, W., and Başar, T. (2017), "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game", *Proceedings of the 2017 IEEE international conference on communications (ICC)*, IEEE, May, pp.1-6

Shayesteh, B., Hakami, V., and Akbari, A. (2020), "A trust management scheme for IoT-enabled environmental health/accessibility monitoring services", *International Journal of Information Security*, Vol.19, No.1, pp.93-110.

Souissi, I., Azzouna, N.B., and Said, L.B. (2019), "A multi-level study of information trust models in WSN-assisted IoT", *Computer Networks*, Vol.151, pp.12-30.

Statista (2021), "Number of web application attacks in the Caribbean 2019", [online] Available at: https://www.statista.com/statistics/1058898/internet-application-attacks-caribbean-countries/ [Accessed 22 Feb. 2022]

Taheri, M., Khorasani, K., Shames, I., and Meskin, N. (2020), "Cyber attack and machine induced fault detection and isolation methodologies for cyber-Physical systems", arXiv preprint arXiv:2009.06196.

Tahri, A., Hassaine, S., and Moreau, S. (2018), "A hybrid active fault-tolerant control scheme for wind energy conversion system based on permanent magnet synchronous generator", *Archives of Electrical Engineering*, Vol.67, No.3, pp.485-497.

Tamronglak, S., Horowitz, S.H., Phadke, A.G., and Thorp, J.S. (1996), "Anatomy of power system blackouts: preventive relaying strategies", *IEEE Transactions on Power Delivery*, Vol.11, No.2, pp.708–715.

Tang, D., Pham, C., Chinen, K.I., and Beuran, R. (2017), "Interactive cybersecurity defense training inspired by web-based learning theory", *Proceedings of the 2017 IEEE 9th International Conference on Engineering Education (ICEED)*, IEEE, November, pp. 90-95

The Tico Times (2019), "System failure causes power outage through much of Central America", *Costa Rica News*, [online] Available at: https://ticotimes.net/2019/09/16/system-failure-causes-power-outage-through-much-of-central-america [Accessed 18 Oct. 2021].

Thirumarimurugan, M., Bagyalakshmi, N., and Paarkavi, P. (2016), "Comparison of fault detection and isolation methods: A review", *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, IEEE, January, pp.1-6

Toapanta, S.M.T., Jaramillo, J.M.E., and Gallegos, L.E.M. (2019), "Cybersecurity analysis to determine the impact on the social area in Latin America and the Caribbean", *Proceedings of the 2019 2nd International Conference on Education Technology Management*, December, pp.73-78.

Trinidad and Tobago Guardian (2020), "Pipe failure shuts down Methanol Holdings", [online] *Trinidad and Tobago Guardian*, Available at: https://www.guardian.co.tt/news/pipe-failure-shuts-down-methanol-holdings-6.2.1163390.6287bda987 [Accessed 22 Feb. 2022].

Trinidad and Tobago Guardian (2021a), "Power restored after island-wide blackout on Tobago", *Trinidad and Tobago Guardian*, [online] 27 January, Available at: https://www.guardian.co.tt/news/power-restored-after-islandwide-blackout-on-tobago-6.2.1281486.67593ac53b [Accessed 22 Feb. 2022].

Trinidad and Tobago Guardian (2021b), "T&TEC: Power outages due to problems at power plant", *Trinidad and Tobago Guardian*, [online] 22 Dec. Available at: https://www.guardian.co.tt/news/ttec-power-outages-due-to-problems-at-power-plant-6.2.1430576.f36eb8bb59 [Accessed 22 Feb. 2022].

Trinidad and Tobago Weather Center (2019), "Two Power Dips across Trinidad Due to DESALCOTT", [online] Available at: https://ttweathercenter.com/2019/05/29/two-power-dips-across-trinidad-due-to-desalcott/ [Accessed 18 Oct. 2021].

T&TEC (2022), "Update on Restoration efforts after island wide outage", Trinidad and Tobago Electricity Commission, [online] 17 Feb. Available at: https://www.facebook.com/TTElectricityCommission/photos/a.475554313074390/991520711477745/ [Accessed 22 Feb. 2022].

TTCSIRT (2020), "Increase in ransomware attacks targeting public and private entities in Trinidad and Tobago", [online] Trinidad and Tobago Cyber Security Incident Response Team, Available at: https://ttcsirt.gov.tt/ransomware-alert-2020/ [Accessed 22 Feb. 2022].

TTT News (2021), "T&TEC Restores Power after Islandwide Outage", [online] TTT News. Available at: https://www.ttt.live/ttec-restores-power-after-islandwide-outage/ [Accessed 22 Feb. 2022].

Wang, J., Yao, Y., Zhang, G., and Li, F. (2020), "Defense method of ruby code injection attack based on instruction set randomisation", *Proceedings of the 8th International Conference on Computer and Communications Management*, July, pp.63-67.

Wang, K., Tian, E., Liu, J., Wei, L., and Yue, D. (2020), "Resilient control of networked control systems under deception attacks: A memory-event-triggered communication scheme", *International Journal of Robust and Nonlinear Control*, Vol.30, No.4, pp.1534-1548.

Wang, Z., Rodrigues, M., Theilliol, D., and Shen, Y. (2015), "Actuator fault estimation observer design for discrete-time linear parameter-varying descriptor systems", *International Journal of Adaptive Control and Signal Processing*, Vol.29, No.2, pp.242-258.

WASA (2018), Emergency Shutdown at Point Lisas Desalination Plant", Water and Sewerage Authority, Available at: https://www.facebook.com/240271669431165/photos/pb.100064440051769.-2207520000../921927014598957/?type=3 [Accessed 22 Feb. 2022].

Wei, D. and Ji, K. (2010), "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights", Proceedings of the 2010 3rd International Symposium on Resilient Control Systems, IEEE, August, pp.15-22

Willems, C., Klingbeil, T., Radvilavicius, L., Cenys, A., and Meinel, C. (2011), "A distributed virtual laboratory architecture for cybersecurity training", *Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions*, IEEE, December, pp. 408-415

Wu, J., Peng, C., Yang, H., and Wang, Y.L. (2022), "Recent advances in event-triggered security control of networked systems: A survey", *International Journal of Systems Science*, Vol.53, No.12, pp.2624-2643.

Wu, J., Peng, C., Zhang, J., Yang, M., and Zhang, B.L. (2020), "Guaranteed cost control of hybrid-triggered networked systems with stochastic cyber-attacks", *ISA transactions*, Vol.104, pp.84-92.

Xie, C., Wang, J., Zhang, Z., Ren, Z., and Yuille, A. (2017), "Mitigating adversarial effects through randomisation", arXiv preprint arXiv:1711.01991.

Yin, S., Gao, H., Qiu, J., and Kaynak, O. (2016), "Adaptive fault-tolerant control for nonlinear system with unknown control directions based on fuzzy approximation", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol.47, No.8, pp.1909-1918.

Yuan, Y., Liu, X., Ding, S., and Pan, B. (2017), "Fault detection and location system for diagnosis of multiple faults in aeroengines", *IEEE Access*, Vol.5, pp.17671-17677.

Yuan, Y., Sun, F., and Liu, H. (2015), "Resilient control of cyber-physical systems against intelligent attacker: A hierarchal stackelberg game approach", *International Journal of Systems Science*, Vol.47, No.9, pp.2067-2077.

Yun, J., Park, K.W., Koo, D., and Shin, Y. (2020), "Lightweight and seamless memory randomisation for mission-critical services in a cloud platform", *Energies*, Vol.13, No.6, pp.1332.

Zhang, Q., Yan, H., Zhang, H., Chen, S., and Wang, M., (2020), H ∞ control of singular system based on stochastic cyber-attacks and dynamic event-triggered mechanism", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol.51, No.12, pp.7510-7516.

Zhao, L., Xu, H., Zhang, J., and Yang, H. (2022), "Resilient control for wireless cyber-physical systems subject to jamming attacks: A Cross-layer dynamic game approach", *IEEE Transactions on Cybernetics*, Vol.52, No.4, pp.2599-2608.

Authors' Biographical Notes:

Amir Mohammed *received his BSc and MASc in Electrical and Computer Engineering with a major in Control Systems from The University of the West Indies (UWI), St Augustine. He is currently a PhD Candidate in Electrical and Computer Engineering at the UWI. His interests include Cyber Physical Systems, Resilient Control and Fault Tolerant Control.*

Lincoln Marine *received his BSc in Electrical and Computer Engineering with a major in Control Systems and Communication Systems from The University of the West Indies (UWI), St Augustine. His interests include Fuzzy Logic Control and Machine Learning.*

Craig J. Ramlal *received his B.Sc(e) in Electrical and Computer Engineering, MASc in Electrical and Computer Engineering (Control Systems Major) and his PhD in Electrical and Computer Engineering split site with The University of the West Indies, Trinidad and Tobago and the King Fahd University of Petroleums and Minerals, Dhahran, Saudi Arabia. His research focus includes Intelligent and Robust Control Techniques and Machine Learning with applications in Autonomous Robotics, Medical Technology, Education and Power, Process and Communication Systems.*

Fasil Muddeen *is a Lecturer in the Department of Electrical and Computer Engineering at The University of the West Indies. His areas of research include the acoustics of the steelpan, digital signal processing, electronics, measurement and instrumentation. Dr. Muddeen is a registered engineer with the Board of Engineering of Trinidad and Tobago, a Fellow of the Association of Professional Engineers of Trinidad and Tobago, a Member of the IEEE and a former Chairman of the IEEE Trinidad and Tobago Section.*

■