Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

Cornelia Skaga

# Energy Control of Complex Cyber-Physical Microgrids: Robustness against Cyber Attacks

Master's thesis in Energy and Environmental Engineering
Supervisor: Gilbert Bergna-Diaz
June 2022

NTNU
Norwegian University of Science and Technology

Cornelia Skaga

# Energy Control of Complex Cyber-Physical Microgrids: Robustness against Cyber Attacks

Master's thesis in Energy and Environmental Engineering
Supervisor: Gilbert Bergna-Diaz
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Electric Power Engineering

NTNU
Norwegian University of
Science and Technology

# Preface

*The most enjoyable year of my education has been this last year, a lot due to this master. I have gained a wider understanding of electrical power systems and I have really enjoyed focusing on operation and control in order to optimize the utilization of renewable electric energy.*

*I wish to direct a huge thank you to my supervisor, Professor Gilbert Bergna-Diaz for his support and guidance throughout this thesis. Gilbert has brought knowledge, engagement, and has been dedicated to helping me understand new topics and approaches. This includes new basic concepts helping me to independently continue the research. He has helped me to gain an even wider understanding of the theory presented in this thesis as well as other concepts related to my education. I would love to work with him again if I were to continue with scientific research.*

*I would also like to thank Babak Abdolmaleki who wrote the article on which I based my model of the direct-current microgrid. He has guided and supported me, band challenged me in order to extend the use of all these new concepts and approaches to the point where I independently was able to pursue further work. He has also been very helpful in regard to simulations and presenting the most basic concepts so that I was able to simulate even more complex systems at a later stage.*

*Additionally, I would like to thank my student colleagues that I have been with every day at the university. We have had great discussions, good laughs and it has been a joy and inspiration to see them every day.*

# Abstract

This master's thesis presents an overview of the modelling and design of complex cyber-physical (CP) microgrids (MGs), further extending the work carried out in the associated specialization project. More precisely, the closed loop CP microgrid is first modelled with the port Hamiltonian (pH) formalism, emphasizing the energy preservation and dissipation within the system dynamics, as a starting point for an *energy-based control* design. The dynamics of the electrical network are first presented as a network consisting of distributed generating units, converters, RL-transmission lines, capacitors, power consuming loads and associated inductance's of the devices. Following a hierarchical control perspective, the power generating units have a *decentralized* primary control behaving according to a droop characteristic, measuring the current and regulating the voltage in order to limit the deviations from the pre-defined nominal voltage. Consequently, the primary controller ensures sub-optimal operation of the MG and is shown to be globally asymptotically stable with respect to a new equilibrium point. However, the controller is not able to restore the initial operating conditions and the ability to steer the MG to desired optimal operation is stymied. Motivated by this shortcoming, an outer loop *distributed* secondary controller is proposed, allowing for optimal operation of the MG.

The physical layer of the CP MG is first mathematically modelled by interconnecting generating units, transmission lines and power consuming loads through (skew-symmetric) power preserving interconnections. This model of the physical network characterizes the electrical power system and is shown to admit a pH representation, facilitating the secondary outer loop control design and interconnected MG.

Secondly, the distributed control network dynamics are characterized by the consensus protocol. It is by exploiting the communication between the neighbouring generating units that the MG is able to operate as desired. Hence, this additional distributed control network constitutes the cyber layer of the cyber-physical MG due to the use of communication. It is shown that the cyber network admits a pH representation – in a similar fashion as the electrical network.

The control objectives are then defined, and the MGs secondary controller is implemented with the intention of bringing the system to desired optimal stable operations while satisfying the two control objectives: *proportional current-sharing* and *average voltage regulation*. Proportional current-sharing is ensured by solving a convex optimization problem, formulated with the objective function summarizing the cost of generation. Lagrangian duality is then applied in order to rewrite the problem formulation and solve the convex optimization problem with the Karush-Kuhn-Tucker conditions. The secondary controller is then implemented with dynamics based on the stationary conditions of the optimization problem, thereby providing proportional current-sharing. Average voltage regulation is guaranteed by adding weightings in the interconnections between the two networks, ensuring that the weighted sum of all the generating unit's voltages is equal to the pre-defined nominal voltage of the MG.

The two layers (cyber and physical) are then interconnected through an interconnection pattern–including the added weightings and modified dissipation–constituting the final cyber-physical MG. The overall system in closed loop–with the primary and secondary controllers–is shown to globally asymptotically stabilize to an optimal equilibrium point. This is concluded by using an incremental energy modelling and Lyapunov's stability method to obtain a generalized stability certificate valid for any CP MG admitting linear dynamics.

However, the use of communication links in the cyber layer makes the control system prone to cyber attacks. Cyber attacks perturbing the power systems may threaten the control performance and thereby the optimal operations of the MG. The cyber attacks may be infiltrating the control dynamics in different locations, thereby causing different operational problems depending on where the attack intrudes. In this thesis, the cyber-physical microgrid is analysed with respect to three different types of cyber attacks maligning the control operations of the MG. The problems emerging from these attacks are then studied with respect to the system's ability to still achieve the desired optimal equilibrium, and capacity to always guarantee stable operations of the MG. Unfortunately, the initial control structure could not always comply with the desired objectives, when subject to a cyber attack. Motivated by this drawback, a resilient control modification is proposed as the main result of this thesis, capable of almost completely mitigating the negative consequences of the attacks.

The final secondary controller is concluded resilient with respect to a variety of cyber threats, regardless of where, when and how the attacks intrude. However, the controller is not robust against the very discrete implemented *stealth attacks*, and the controller needs to be further modified in order to ensure complete novel robustness, while simultaneously ensuring optimal steady state operation.

# Sammendrag

Denne masteroppgaven sammenfatter modellering og design av komplekse cyber-physical (CP) mikro-nettverk (MGs) som tidligere presentert i tilhørende prosjektoppgave. Port Hamiltonian teori er brukt i modelleringsprosessen, altså modellert ved å studere systemets energi strømninger og - bevaring, med hensikt å etablere grunnlaget for å designe et kontrollsystem ved bruk av energi-basert kontroll design. Nettverket er først presentert som en sammenkobling av distribuerte genererende enheter, omformere, overføringslinjer med resistans og induktans, kondensatorer, strøm-forbrukende enheter og individuell induktans assosiert til de ulike enhetene. Deretter er nettverkets kontrollsystem formet ut i fra et hierarkisk kontroll perspektiv der de generende enhetene først vil bli utstyrt med primær lokal spenningsfall-kontroll. Formålet er å begrense spenningsfallet fra den forhåndsdefinerte nominelle spenningen, ved å måle de genererte strømmene som deretter brukes til å regulere spenningen og differansen. Den primære kontrollkonfigurasjonen sørger for suboptimal drift av micronettverket, bekreftet til å tilfredsstille global asymptotisk stabilitet omkring systemets likevektspunkt. Spenningskontrolleren er derimot ikke kapabel til å rekonstruere de opprinnelige og optimale system-betingelsene, og evnen til å styre nettverket til ønsket likevektspunkt, er enda ikke oppnåelig. Dette motiverer videreutviklingen av kontrollsystemet som innebærer implementering av en sekundær ytre kontrollsløyfe med et distribuert kontrollsystem, for å sikre optimal drift av nettverket.

Nettverkets sekundære kontrollsystem består av fysiske- og online forbindelser mellom de genererende enhetene som respektivt danner det fysiske nivået (physical layer) og online nivået (cyber layer) av CP MGs. Det fysiske nivået karakteriserer det elektriske kraftnettverket og er først modellert ved å koble de genererende enhetene, overføringslinjene og strøm-forbrukende enheter gjennom skjev-symmetriske kraftbevarende forbindelser. De kombinerte CP MGs er deretter bevist å komplimentere pH system representasjon, som er en viktig forutsetning når sekundær kontrolleren skal modelleres. Sekundær kontrolleren implementeres med hensikt om å rekonstruere de initiale system-betingelsene, definert i likevektspunktet når kontrollmålene: *proporsjonal strøm-fordeling* og *gjennomsnittlig spennings regulering* er møtt. Proporsjonal strøm-fordeling er oppnådd når kontrollsystemet er designet slik at det tilfredsstiller løsningen av det konvekse optimeringsproblemet, formulert med objektiv funksjon som summerer genereringskostnadene. Lagrange dualitet er deretter brukt for å omskrive problemet slik at optimerings algoritmen kan løses med Karush-Kuhn-Tucker (KKT) betingelsene. Kontrollsystemet kan deretter modelleres for å tilfredsstille denne løsningen og dermed sikre proporsjonal strøm-fordeling. Gjennomsnittlig spenningsregulering er sikret ved å legge til vektinger i forbindelsene mellom online nivået og det fysiske nivået. Den vektede summen av alle de generende enhetenes spenninger vil da tilsvare den forhåndsbestemte nominelle spenningen slik at gjennomsnittlig spenningsregulering er møtt.

De to kontrollmålene er nå etablert, og dynamikken til det distribuerte kontrollsystemet kan implementeres heretter. En konsensus-protokoll er brukt for å modellere hvordan de genererende enhetene kommuniserer online med sine nabo-enheter med mål om å etablere en felles enighet om det optimale driftsnivået. Mot slutten av denne seksjonen er det bevist at online kontrolleren komplimenterer pH system-representasjonen på lik linje med det fysiske nivået, og de to nettverkene kan kobles gjennom vektede forbindelser og modifisert energi-basert sekundær kontroll. For å ferdigstille modellen av det sammenkoblede nettverket må dynamikken til den modifiserte energi-baserte sekundær kontrolleren innføres. Den ytre kontrollsløyfen blir dermed lukket og kontrollsystemet er vist å inneholde både primær og sekundær-kontrollere. En stabilitetsanalyse er deretter utført og det blir konkludert at nettverket stabiliserer seg rundt det optimale likevektspunket ved bruk av teoriene *inkrementell energi modellering* og *Lyapunov stabilitets teorem*. Stabilitetsanalysen sertifiserer et generalisert stabilitetssertifikat som er verifisert for alle nettverk som bevilger lineær dynamikk.

Ulempen med at den sekundære kontrolleren bruker online kommunikasjon er at kontrolleren derfor er utsatt for cyber-angrep. Angrepene truer kontrollprestasjonen som kan forhindre optimal drift av nettverket. Cyber-angrepene kan infiltrere flere steder i dynamikken til kontrollsystemet og vil dermed påvirke kontrollytelsen på ulike måter. I denne oppgaven vil CP MGs bli analysert som et forstyrret nettverk med hensyn til tre potensielle cyber-angrep som kan ødelegge optimal drift. Ulempene forårsaket av disse angrepene er deretter analysert med tanke på evnen til å oppnå stabil–og optimal–drift av nettverket, altså stabilitet samtidig som de to definerte kontrollmålene er møtt. Det er vist, i denne masteren, at den foreslåtte kontrollstrukturen ikke alltid evner å overholde de ønskede kontrollmålene når systemet er under angrep. På bakgrunn av denne konklusjonen forsøkes det å modellere et motstandsdyktig kontrollsystem kapabel i å tilnærmet fullstendig fjerne effekten av cyber-angrepene og dermed sikre optimal drift uavhengig av potensielle angrep.

Det endelige kontrollsystemet er vist motstandsdyktig med hensyn til et mangfold av cyber-angrep uavhengig av hvor, når eller hvordan de infiltrerer sekundær-kontrolleren. Unntaket av de veldig diskret implementerte *Stealth* angrepene og det foreslåtte kontrollsystemet må derfor videre modifiseres for å oppnå fullstendig robusthet mot alle typer cyber angrep.

# List of Abbreviations

| | |
|---|---|
| **AC** | Alternating-Current |
| **BIBS** | Bounded Input Bounded State |
| **CbI** | Control by Interconnection |
| **CP** | Cyber-physical |
| **CPL** | Constant Power Loads |
| **DC** | Direct-Current |
| **DG** | Distributed Generator |
| **DoS** | Denial of Service |
| **FDI** | False Data Injection |
| **ISS** | Input-to-State Stable |
| **KCL** | Kirchhoff's Current Law |
| **KKT** | Karush-Kuhn-Tucker |
| **KVL** | Kirchhoff's Voltage Law |
| **LEC** | Local Energy Community |
| **MG** | Microgrid |
| **MIMO** | Multiple Inputs Multiple Outputs |
| **MITM** | Man-In-The-Middle |
| **PB** | Passivity Based |
| **PBC** | Passivity Based Controller |
| **PI** | Proportional Integral |
| **pH** | port Hamiltonian |
| **RE** | Renewable Energy |
| **RES** | Renewable Energy Sources |
| **RL** | Resistance (R) Inductance (L) |
| **SG** | Smart Grid |
| **TL** | Transmission Line |
| **ZIP – Loads** | Constant Impedance (Z), Constant Current (I), Constant Power (P) - Loads |
| **ZI – Loads** | Constant Impedance (Z), Constant Current (I) - Loads |

# Contents

# 1 Introduction

This master's thesis includes the modelling and design of complex cyber-physical (CP) microgrids (MGs) and the study on how to design a resilient control system robust against cyber attacks. The MGs are designed as autonomous direct current (DC) MGs motivated by their profitable abilities to effectively implement renewable energy sources in electrical power systems. Additionally, they facilitate electrification in local areas which again improves sustainable electrical power utilization by reducing potential transmission losses.

The model of the cyber-physical MGs is based on Babak Abdolmaleki's publication *Distributed Control and Optimization of DC Microgrids: A Port-Hamiltonian Approach* [1]. According to this methodology, the MG controllers are designed based on energy principles, by first assessing how the energy is preserved and dissipated in the system–and its role in the system dynamics–and subsequently utilizing these energy principles for assessing the stability. More precisely, the control system is designed to ensure stable operations of the DC microgrid (MG) while aiming to satisfy the pre-defined control objectives at steady state. Following a hierarchical control structure, a stable operation can be initially ensured by only implementing in each unit a decentralized primary control. However, since we are interested in optimizing the operation of the MG, the desired control objectives are ensured by implementing a distributed control system. This secondary controller exploits the communication between the neighbouring generating units with the intention of establishing the units individual requirements bringing the MG to operate as desired. Due to the communication, the distributed control system constitutes a cyber layer inherently prone to cyber attacks. In turn, the potential cyber attacks may weaken the performance of the MG, and prevent the controllers ability to satisfy the control objectives. Consequently the stability of the system may be affected by the cyber attacks and the MG is compromised, not able to operate under the desired conditions. In order to ensure that the the DC MG is performing optimally in regards to the pre-defined objectives, this thesis extends the result presented in [1] by proposing a resilient energy-based controller capable of bringing the system to operate as close as possible to the desired optimal steady state operating point, while being subject to different types of cyber attacks. Finally, the effectiveness of the proposed controller is independent of the number of generating units and grid topology for any DC microgrid admitting linear dynamics.

## 1.1 DC Microgrid

Microgrids are a relatively new development that have gained extensive attention in the last years as a solution that achieves profitable and effective renewable energy (RE) management. They are either autonomous direct-current (DC) or alternating-current (AC) multi-agent systems, where the agents often are implemented as distributed generators (DGs) located close to the loads [2]. The DGs are effectively interfaced with the grid through power electronic converters and are interconnected as a microgrid (MG) [1].

The study of multi-agent systems, grouped as microgrids, was first introduced in 2001 in the IEEE PES WM Panel and have since been studied as a configuration to achieve energy efficiency, minimization of overall energy consumption, reduced environmental impacts and improvement of energy system reliability [3]. The ability to operate in islanded mode facilitates the electrification in local areas, enhancing technical infrastructure to support Local Energy Communities (LEC) as well as being a vital building block for the composition of Smart-Grids (SGs). Islanding is a operational state in which a portion of the power grid, or a microgrid, gets disconnected from the utility grid where the disconnected grid is independently able to maintain the grid operations such as meeting the load demand and operate at the necessary voltage and power level [4]. IEEE has defined the microgrid standard as: *A group of interconnected loads and distributed energy resources with clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid and can connect and disconnect from the grid to enable it to operate in both grid-connected or island modes*[5].

The implementation of direct-current MGs has gained extensive attention the last years, as they are easier to control an operate while integrating more green technologies [1] such as photovoltaic panels, fuel cells, modern electronic loads (e.g. electric appliances, LED's and electric vehicles [6]) and energy storage systems [7]. The majority of renewable energy sources (RES) and electrical loads have DC electrical nature depending only on the current and voltage variables. Compared to AC microgrids the control mechanism do not need to account for frequency, reactive power, power quality or three-phase balanced signals in order to regulate the system [7][6]. The DC grid will therefore have simpler dynamics, easing the control and management [1]. However, increased applicability of DC microgrids lead to challenges related to modeling and control techniques as they are new developments and consequently have been less studied and researched [7].

## 1.2 Control Configurations of DC Microgrids

In order to achieve the desired operational objectives of microgrids, several *hierarchical control* configurations have been researched and proposed. Hierarchical control is a strategy that standardizes the operation and functionality of the micorgrid which includes implementing the three level controllers *primary*, *secondary* and *tertiary* with separate time scales. The primary control is typically droop based implementing a proportional controller in the closed loop of the DGs facilitating quick stabilization of the DG by controlling the voltage and current output. The primary control will therefore often have a decentralized structure, controlling the units locally with no communication links between the units. The primary controller is implemented to ensure stable and reliable operations. In addition, the primary control facilitates a control system that is robust against communication failure; i.e., the system will operate sup-optimally and achieve steady state regardless of perturbation in the communication system. The main objective of the primary controller is to limit the deviations and stabilize the system. The secondary control level is then implemented to compensate for the deviations; i.e., restoring the operating conditions prior to the deviations. The secondary controller will therefore operates at a slower time scale than the primary control. The final tertiary control level is implemented in order to achieve optimal operation and power management within the microgrid. Both the secondary and tertiary control levels are typically distributed and centralized respectively, sharing the information between the DGs through communication links [7]. In this thesis the control is designed and implemented to break–to a certain extent–this control hierarchy by merging primary, secondary and tertiary control level, introduced as one control scheme.

The centralized control strategies are non-scalable and non-robust to single point of failure [7] which might bring the whole system to failure. Decentralized control schemes are more scalable but not capable to achieve the optimal grid objectives. Hence, the distributed control scheme is implemented in this thesis as a compromise between the centralized and decentralized strategies. The research on this topic and its different implementation methods have gained extensive interest in the recent years, streamlining the implementation of RES, energy storage systems and electric loads into the power system [1] enhancing the flexibility, scalability and reliability of the grid [2]. The distributed control systems require communication links, however they are only interconnected between neighbouring units using peer-to-peer communication, configuring a more space communicating network topology compared to the centralized configuration with high bandwidth. This creates a scalable control system that is independent of the knowledge of the whole microgrid [8]. The consensus protocol is one of the proposed communication techniques used to achieve cooperatively control of a multi agent system; i.e., controlling the DGs in order to achieve the optimal objectives of the system.

The most common control objectives of DC microcrids are voltage regulation and proportional current-sharing. Voltage regulation is required to ensure proper functioning of the connected loads operating within specified power limits. Current-sharing allows the DGs to proportionally share their generation capacity, preventing overstress in the distributed units facilitating safety and stable operations of the network [8]. The DC MG modelled in the associated specialization project is further studied in this thesis. The specialization project initiated research on an energy-based distributed control system and this thesis extends the work by i) implementing distributed and optimal (PI-)controllers, ii) assessing the effects of three different types of potential cyber attacks, and iii) robustifying the control strategy against these attacks. To be exact, the desired control objectives of the microgrid are defined as proportional current-sharing and average voltage regulation. The first objective is based on sharing the cost of generation between the generating units, exploiting online communication in order to achieve one consensus value for the incremental costs of generation. In order to ensure these two desired control objectives for the cyber-physical MG, one additional control objective is presented in this thesis. The distributed control system needs to incorporate a resilience property: i.e., ensuring that the MG is robust against communication and system failures due to potential cyber attacks.

## 1.3 Scope and Objectives

Due to the reliance of the secondary control configuration on a distributed communication network, this thesis aims to design a novel control system ensuring that the MG converges to a steady state equilibrium while satisfying the three control objectives: *Equal incremental costs*, *Average voltage regulation* and *Resilience against cyber threats*. The cyber-physical DC MG studied in this thesis is based on the model presented in the associated specialization project and the final closed loop control system is further modified in this thesis aiming to simultaneously ensure steady state optimal operations with respect to the three defined control

objectives. The main objectives of this thesis are therefore presented as follows:

**Thesis Objective 1** : *Modelling of a cyber-physical (linear) DC microgrid and obtaining the generalized stability certificate ensuring optimal operations*

The first thesis objective, presented above, focuses on energy modelling using the port-Hamiltonian formalism of a generalized linear cyber-physical MG with the goal of facilitating the search for stability certificates, which are in turn based on Lyapunov's direct method.

**Thesis Objective 2** : *Proposing a novel resilient control strategy ensuring robustness against all cyber attacks*

Towards this end, the resilience is tested by first studying how potential cyber attacks may intrude, what disadvantages they may cause and the effect of tuning the control parameters to a sufficient resilient threshold. The resilience is defined sufficient when the influence of the attacks is reduced to the point where the perturbed system is operating as unforced: i.e., to the point where the first thesis objective is satisfied. The controller is further modified and tuned until the disadvantages caused by the attacks may be disregarded and it is possible to conclude that the CP MG operates as unforced while being exposed to cyber threats.

Combining the two thesis objectives provides one final thesis objective defined as *obtaining a novel resilient distributed secondary control configuration for linear DC microgrids with global stability certificates.*

### 1.3.1 Limitation of Scope

The first part of this thesis includes the energy modelling of the completely linear DC MG. The converters are implemented in each DG, modelled as zero-order converters without specified inherent dynamics. The use of linear zero-order converters ensures generality where the obtained stability certificates are valid for any other linear systems. It is therefore easily shown that other linear converters such as *buck/boost* or *bidirectional* may be implemented *mutatis mutandis* where the conclusions of this thesis are equally valid. Additionally, the constant power loads (CPL)–often implemented in regular ZIP-loads–are disregarded as they contribute with negative damping, inherently destabilizing the system with their nonlinear dynamics. The obtained generalized stability certificates are then proven valid for only linear systems admitting the same dynamics. However, as the Lyapunov stability method is still used to carry out the analysis, it is expected that this will serve as a useful starting point for further studies focusing on the neglected nonlinear dynamics.

When the model of CP MG is completed, the controller is assessed with respect to stability and ability to ensure the desired optimal operations while being prone to all potential cyber attacks. However, there are only three types of cyber threats studied in this thesis. The attacks are implemented as perturbations in both of the two modelled networks and in the interconnections between them, presenting the threats perturbing in all the three main units of the model: i.e., representing the primary attack locations. However, as long as the controller uses communication, the cyber attacks may perturb in multiple locations beyond what is presented in this thesis. In order to limit the number of necessary system analyses, the thesis concludes that it is sufficient to study the drawbacks caused by the three attacks. Equally, the sufficient resilience strategy is only tested when the three attacks occur. If the final conclusion is validated for the studied cyber threats, it is assumed to be valid for any type of cyber threat, regardless of the location of the attack,

The primary focus of this thesis is on energy modelling and control, with respect to stability and the ability to ensure optimal operations while the power system is subject to cyber attacks. The performed analyses will therefore not include the transient control performance, as this is rather left for further studies. The performance of the controller may then be assessed from a dynamic perspective assessing e.g. the transient response of the states when the attacks intrude or the state responses when potential resilient tuning strategies are applied. Hence, when the case specific MG is simulated as the perturbed system, only the control objectives are presented as the relevant plotted values. The plots regarding the states of the DGs, transmission lines, loads and controller states are not implemented in this thesis as they correspond to this the performance analysis left for further studies.

**Remark**: With some abuse of standard terminology, this thesis refer to *control performance* as the ability of the controller to achieve the optimal steady state equilibrium. This is deemed – even though the terminology often is reserved to transient performance – as this thesis studies the ability of the controller to comply with the control objectives at the steady state equilibrium.

### 1.3.2 New Contribution

The first part of this thesis gives an overview of the modelling performed in the specialization project and completes the modelling of the passivity based PI-controller. Due to the nature of the project this first part follows the energy modelling of a DC MG presented in Babak Abdolmaleki's publication [1]. However, the subsequent parts of this thesis implements different cyber attacks independently modelled and influenced by the literature. Hence, the proposed distributed control configurations presented in [1] is now assessed with respect to potential threats and the performance of the controller is tested beyond what is presented in the article. Additionally, the last section includes control modifications of the proposed controller. Hence, the final contribution of this thesis is the study on how to model appropriate cyber attacks, performance assessment of the proposed controller subject to cyber threats, robustness analyses, and a modified controller optimizing the control operations when arbitrary cyber attacks are present.

## 1.4 Thesis Overview

The outline of the thesis is divided into four main parts *Part: A, B, C* and *D* with the following content:

*Part A: Complex Cyber-Physical Microgrids: Under Nominal Conditions* presents an overview of the cyber-physical DC microgrid modelled in the associated specialization project. The final closed loop control system is then implemented as the passivity based controller aiming to ensure steady state stability and optimal operations with respect to the pre-defined control objectives of the DC MG.

*Part B: Complex Cyber-Physical Microgrids: Under Cyber Attacks* includes a literature review of potential cyber threats and associated detection and mitigating approaches. The theoretical study on perturbed systems exposed to cyber threats is then presented with additional theory regarding bounded attacks and bounded/limited stability properties. An in depth analysis of the system operational destruction entailed by three different cyber attacks is then presented, followed by a proposed resilient control strategy, aiming to reduce the destruction caused by the attacks. The theoretical conclusions are additionally validated by simulating a case specific cyber-physical DC MG subject to three cyber attacks, and the resilient tuning strategy is tested.

*Part C: Cyber Attack Resilient Control Modifications* proposes control system modifications implemented to optimally robustify the resilient controller. The modifications are motivated by the shortcomings of the resilient controller presented in *Part B*. The conclusions are validated by theoretical proofs and by simulations of the case specific cyber-physical DC MG subject to three cyber attacks with resilient control modifications. *Part D: Conclusion* concludes this thesis. Potential further work is then presented as important following studies enhancing the robustness property for a generalized cyber-physical MG aiming to optimize the performance of the controller when potential cyber attacks are present.

*Appendix* provides additional simulations supporting the conclusions presented in the thesis. Supporting theory and conducted proofs are also included as sections previously presented in the associated specialization project. Additional studied theory, used to completely understand the new topics, is also implemented in the *Appendix*.

## Part A:

# Complex Cyber-Physical Microgrids: Under Nominal Conditions

*Part A* of this thesis presents an overview of the DC microgrid modelled in the associated specialization project. The MG is modelled based on energy principles using the port Hamiltonian (pH) formalism to describe the dynamics of the interconnected network. The desired control objectives are established and the distributed control network is proposed as the control solution ensuring the optimal operation of the MG. Furthermore, the inherent dynamics of the control system –which were not modelled in the specialization project –are presented in the last sections of *Part A* where the passivity based PI-controller is implemented, exploiting communication and aiming to ensure both pre-defined control objectives at the steady state equilibrium of the network is proposed.

# 1 Energy Modelling of Electrical Network

The physical layer of the cyber-physical DC MG is first modelled as the electrical power system able to independently operate at steady state. The dynamics of the power generating and power consuming units are first presented where the DGs are modelled with primary droop control converters. Furthermore, the interconnections within the physical layer are presented by using graph theory, initially defining and interconnecting two separate graphs, constituting the final electrical power system. The complete model of the physical layer is lastly presented by using the port Hamiltonian system representation, emphasizing how the system is modelled and interconnected in order to provide power preserving properties within the MG.

The associated specialization project includes Lyapunov stability evaluation of the primary controller ensuring sub-optimal steady state operations of the MG. The proof is based on incremental energy, used in order to ensure that the system converges to the minimum steady state equilibrium point: i.e., converges to the point where the time-dependent state variables equal zero. The final result of the assessment is a generalized stability certificate applicable for any MG admitting linear dynamics.

## 1.1 Electrical Network Modelling

Although the theoretical stability and robustness results of this thesis are valid for any *linear* microgrid with any number of DGs and grid topology, it is still useful to adopt a specific test case for the sake of explanation. Thus, without loss of generality, the case-specific DC microgrid used as a test case in this thesis consists of three main components: four *distributed generators* (DGs) with associated four power consuming *constant impedance (Z)-constant current (I) - loads* (ZI) that are interconnected through five passive *RL-transmission lines* (TLs). Figure 1.1 visualizes the dynamics of an arbitrarily distributed generator, connected to associated power consuming ZI-load. The power producing and generating units are then shown to be interconnected through RL-transmission lines, constituting the rest of the MG.

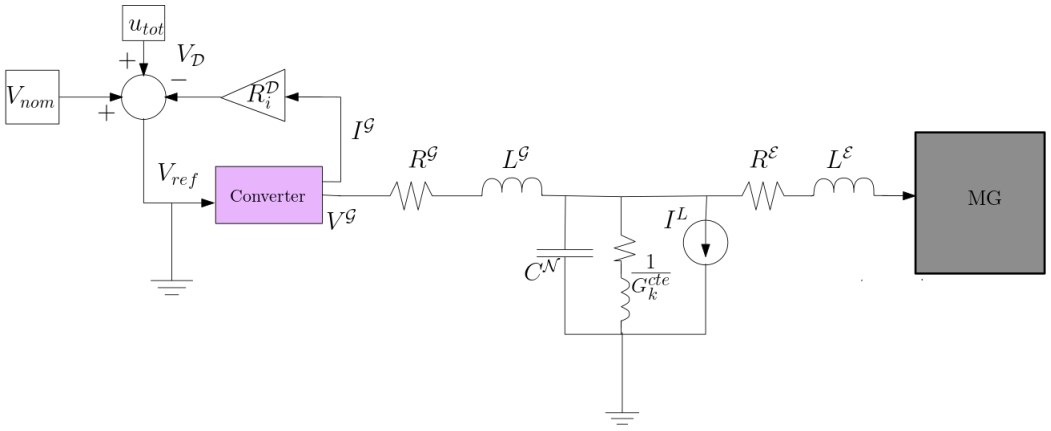


Figure 1.1: Droop controlled DG connected to the rest of the MG through a ZI-load and RL-transmission lines

When only studying the closed loop electrical network, the dynamics displays voltage regulation with primary droop control. The outer loop controller, $u_{tot}$–later defined as the secondary controller– of the cyber layer, is disregarded when the electrical network is modelled. The secondary controller is later implemented when the cyber layer of the MG is modelled. The intrinsic dynamics of each distributed generator provide the primary droop control configuration, facilitating decentralized control of the DC MG limiting voltage deviations with respect to the predefined nominal voltage, $V_{ref} = V_{nom}$. $R_i^D$ is the droop control gain defining the allowable deviation of the generator voltage with respect to the reference voltage. KVL is used on the closed control loop within the DGs and the primary droop control configurations are expressed as:

$$V_i^{\mathcal{G}} = V_i^{ref} = V_{nom} - R_i^{\mathcal{D}} I_i^{\mathcal{G}} + u_{tot}$$

For the case specific MG, used as a didactic example when presenting the motivation behind the designed

generalized cyber-physical MG, the primary droop control characteristics are defined as:

$$V_1^{\mathcal{G}} = V_1^{ref} = V_{nom} - R_1^{\mathcal{D}} I_1^{\mathcal{G}} + u_{tot,1}$$
$$V_2^{\mathcal{G}} = V_2^{ref} = V_{nom} - R_2^{\mathcal{D}} I_2^{\mathcal{G}} + u_{tot,2}$$
$$V_3^{\mathcal{G}} = V_3^{ref} = V_{nom} - R_3^{\mathcal{D}} I_3^{\mathcal{G}} + u_{tot,3}$$
$$V_4^{\mathcal{G}} = V_4^{ref} = V_{nom} - R_4^{\mathcal{D}} I_4^{\mathcal{G}} + u_{tot,4}$$

The DGs are equipped with zero-order linear converters. This implies that the converter is defined without inherent dynamics, always ensuring that the output voltage of the DGs, $V_i^{\mathcal{G}}$, equals the reference voltage. However, other converters may later be implemented and all subsequent proofs are still equally valid as long as the converter admits linear dynamics.

The power consuming loads are modelled as constant impedance, $G_k^{cte}$, and constant current, $I_k^{cte}$, ZI-loads implemented in parallel with a capacitor, $C_k^{\mathcal{N}}$. The loads are modelled based on the structure of the generalized *ZIP-loads* consisting of constant impedance, constant current and a constant power load (CPL). The CPL has the inherent dynamics: $\frac{P^{cte}}{V_i^{\mathcal{N}}}$ i.e., the slope of the power depends on the inverse value of a time varying state variable giving a nonlinear characteristic. The CPL introduces negative damping causing a destabilizing effect, and this thesis disregards this element to work with a linear system for generality and simplicity. KCL is used to obtain the current flowing into the load defined as $I_k^L$: i.e., using KCL on the node connecting the constant impedance and the constant current. The consumed power in the loads is then expressed below where $V_k^{\mathcal{N}}$ represents the voltage induced by the connected capacitor.

$$I_k^L = G_k^{cte} V_k^{\mathcal{N}} + I_k^{cte}$$

The associated equations expressing the loads of the case specific MG is then given below.

$$I_1^L = G_1^{cte} V_1^{\mathcal{N}} + I_1^{cte}$$
$$I_2^L = G_2^{cte} V_2^{\mathcal{N}} + I_2^{cte}$$
$$I_3^L = G_3^{cte} V_3^{\mathcal{N}} + I_3^{cte}$$
$$I_4^L = G_4^{cte} V_4^{\mathcal{N}} + I_4^{cte}$$

The inherent dynamics of the DGs, associated primary voltage control, ZI-loads and RL-transmission lines are finalized in the presentation given in 1.1.2. However, as the final network later is modelled as a cyber-physical MG using graph theory, the interconnections of the physical network also need to be compatible with graph theory. Two initially defined graphs of the electrical system are therefore firstly explained, before the final dynamics of the physical MG are presented.

### 1.1.1 Electrical Network Modelling: Using Graph Theory

Graph theory is used to generalize the model of the MG interconnections with respect to the interactions within the multi-agent system: i.e., studying the system power flows [2]. The objects of the graphs are defined as the *nodes*, which equals the loads in the case specific MG and the interconnections between the nodes are defined as a set of *edges* equal to either the generator edges or the transmission lines in the two graphs. The set of nodes are expressed as $\mathcal{N}_{\mathcal{G}} = \{1, 2, ..., n_{\mathcal{G}}^{\mathcal{N}}\}$. The interconnections between the nodes are represented as a set of edges $\mathcal{E}_{\mathcal{G}} = \{1, 2, ..., m_{\mathcal{G}}^{\mathcal{E}}\}$. The number of nodes, $n_{\mathcal{G}}^{\mathcal{N}}$ defines the order of the graph. The individual node of study is defined as the *vertex object* with edges interconnecting two neighbouring *vertices* [2]. This thesis only considers *strongly connected* and *unbalanced* graphs, meaning that there exists a direct path through the total network from one node to another node and that the number of edges entering and leaving one node is not necessarily equal. The third graph property described in the MG modelling is whether the graph is defined *directed* or *undirected*. A directed graph has edges with a specified direction of flow, whereas the undirected graph has edges with an undefined direction of flow [2]. However, when studying undirected graphs an arbitrary flow direction is defined in order to conduct mathematical analysis on systems including undirected graphs. When graph theory is used in modelling and assessments of electrical networks there are four matrices of interest: *Adjacency matrix*, *Degree matrix*, *Incidence matrix* and the *Laplacian matrix*. In this thesis, the Incidence matrix is mostly used in the electrical modelling of the MG, and the three other matrices are very useful when designing the distributed control network of the cyber-physical MG.

The two individual graphs, presented below, provides the starting point when the case specific MG is modelled. The incidence matrix is used in this section to define the network topology of the two graphs. The incidence matrix, $\mathcal{B}$, contain all the connections between the nodes and the edges in the graph where element $\mathcal{B}_{ij}$ equals 1 if the flow is defined to node $i$ from node $j$, equals -1 if the flow is defined from node $i$ to node $j$. The element equals 0 if there is no connection between the two nodes. The incidence matrix of directed graphs will then describe the real flow path through the network, or only represent one possible arbitrary flow path for the undirected network.

*Graph 1:* $\mathcal{M}^{\mathcal{G}} = (\mathcal{N}_k, \mathcal{G}_i, \mathcal{B}^{\mathcal{G}})$ represents the generating units and the power consuming loads of the DC MG and is presented in Figure 1.2. $\mathcal{N}_k$ is the set of nodes: i.e., set of loads within the MG, represented in both Graph 1 and Graph 2, where $k = \{1, ..., n^{\mathcal{N}_k}\}$, $n^{\mathcal{N}_k} = 4$. $\mathcal{G}_i$ is the set of distributed generators including the generator edges interconnecting the generators and the loads, where $i = \{1, ..., n^{\mathcal{G}_i}\}$, $n^{\mathcal{G}_i} = 4$. The generators are assumed to be power injection components, not absorbing any power and the flow is therefore determined from the generators to the loads. The incidence matrix of *Graph 1*, $\mathcal{B}^{\mathcal{G}} \in \mathbb{R}^{n^{\mathcal{N}_k} \times n^{\mathcal{G}_i}}$, will therefore only contain elements of 1's or 0's. $\mathcal{B}^{\mathcal{G}} \in \mathbb{R}^{4\times4}$ is presented below for the case specific MG.

$$\mathcal{B}^{\mathcal{G}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{1.1}$$

*Graph 2:* $\mathcal{M}^{\mathcal{E}} = (\mathcal{N}_k, \mathcal{E}_j, \mathcal{B}^{\mathcal{E}})$ represents the power consuming loads and associated transmission lines, presented in Figure 1.3. $\mathcal{N}_k$ is the set of nodes defined above, and $\mathcal{E}_j$ is the set of edges i.e the transmission lines, where $j = \{1, ..., n^{\mathcal{E}_j}\}$, $n^{\mathcal{E}_j} = 5$. Graph 2 is undirected, however an arbitrary flow of direction is defined in order to establish the incidence matrix $\mathcal{B}^{\mathcal{E}} \in \mathbb{R}^{n^{\mathcal{N}_k} \times n^{\mathcal{E}_j}}$. For the case specific MG, the incidence matrix $\mathcal{B}^{\mathcal{E}} \in \mathbb{R}^{4\times5}$ is defined as:

$$\mathcal{B}^{\mathcal{E}} = \begin{bmatrix} -1 & 0 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 \end{bmatrix} \tag{1.2}$$

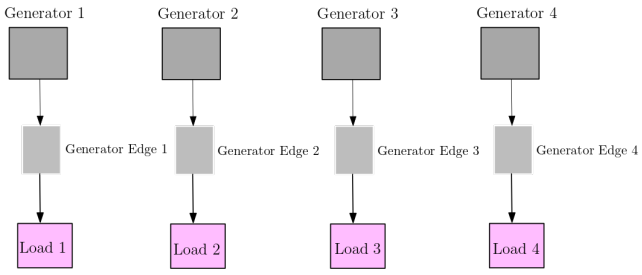


Figure 1.2: Graph 1

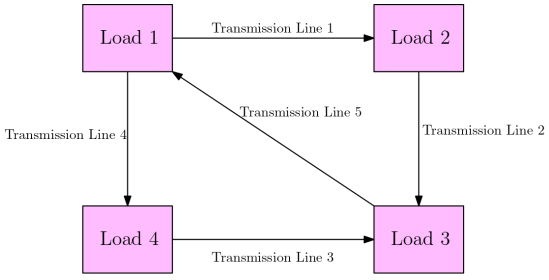


Figure 1.3: Graph 2

### 1.1.2 Dynamics of Electrical Network

Graph theory combined with KVL/KCL used on the dynamics presented in Figure 1.1 are then used to express the dynamics of the interconnected electrical as:

$$L_i^{\mathcal{G}} \dot{I}_i^{\mathcal{G}} = V_i^{\mathcal{G}} - \sum_k b_{ki}^{\mathcal{G}} V_k^{\mathcal{N}} - R_i^{\mathcal{G}} I_i^{\mathcal{G}} \tag{1.3}$$

$$L_j^{\mathcal{E}} \dot{I}_j^{\mathcal{E}} = -\sum_k b_{kj}^{\mathcal{E}} V_k^{\mathcal{N}} - R_j^{\mathcal{E}} I_j^{\mathcal{E}} \tag{1.4}$$

$$\mathcal{C}_k^{\mathcal{N}} \dot{V}_k^{\mathcal{N}} = \sum_j b_{kj}^{\mathcal{E}} I_j^{\mathcal{E}} + \sum_i b_{ki}^{\mathcal{G}} I_i^{\mathcal{G}} - I_k^L \tag{1.5}$$

$$I_k^L = G_k^{cte} V_k^{\mathcal{N}} + I_k^{cte} \tag{1.6}$$

$$V_i^{\mathcal{G}} = V_i^{ref} = V_{nom} - R_i^{\mathcal{D}} I_i^{\mathcal{G}} + u_{tot} \tag{1.7}$$

Equation 1.3 is expressed by applying KVL on the loop connecting the converter, generator edge and the connected load. The dynamics represent the induced voltage in the DGs where $L_i^{\mathcal{G}}$ is the inductance of the $i^{th}$ generator, $V_i^{\mathcal{G}}$ and $I_i^{\mathcal{G}}$ is the voltage and current output and $R_i^{\mathcal{G}}$ is the generator resistance. $b_{ki}^{\mathcal{G}}$ represents the elements in the incidence matrix of Graph 1.

$$L_i^{\mathcal{G}} \dot{I}_i^{\mathcal{G}} = V_i^{\mathcal{G}} - \sum_k b_{ki}^{\mathcal{G}} V_k^{\mathcal{N}} - R_i^{\mathcal{G}} I_i^{\mathcal{G}}$$

For the case specific MG the above equation can be viewed as the set of four equations given below, where the $i$ is replaced with the associated numbered DGs and $k$ is replaced with the connected load to the $i^{th}$ DG.

$$\begin{aligned}
L_1^{\mathcal{G}} \dot{I}_1^{\mathcal{G}} &= V_1^{\mathcal{G}} - V_1^{\mathcal{N}} - R_1^{\mathcal{G}} I_1^{\mathcal{G}} \\
L_2^{\mathcal{G}} \dot{I}_2^{\mathcal{G}} &= V_2^{\mathcal{G}} - V_2^{\mathcal{N}} - R_2^{\mathcal{G}} I_2^{\mathcal{G}} \\
L_3^{\mathcal{G}} \dot{I}_3^{\mathcal{G}} &= V_3^{\mathcal{G}} - V_3^{\mathcal{N}} - R_3^{\mathcal{G}} I_3^{\mathcal{G}} \\
L_4^{\mathcal{G}} \dot{I}_4^{\mathcal{G}} &= V_4^{\mathcal{G}} - V_4^{\mathcal{N}} - R_4^{\mathcal{G}} I_4^{\mathcal{G}}
\end{aligned}$$

Equation 1.4 represent the induced voltage in the transmission lines, obtained by applying KVL on the loop connecting the loads and the transmission line of interest. $L_j^{\mathcal{E}}$ and $R_j^{\mathcal{E}}$ are the inductance and resistance in the lines, and $V_k^{\mathcal{N}}$ is the voltage over the capacitors in the two connected loads. $I_j^{\mathcal{E}}$ is the current flowing through the lines and $b_{kj}^{\mathcal{E}}$ represents the elements in the incidence matrix of Graph 2.

$$L_j^{\mathcal{E}} \dot{I}_j^{\mathcal{E}} = -\sum_k b_{kj}^{\mathcal{E}} V_k^{\mathcal{N}} - R_j^{\mathcal{E}} I_j^{\mathcal{E}}$$

For the case specific MG the above equation can be viewed as the set of five equations presented below.

$$\begin{aligned}
L_1^{\mathcal{E}} \dot{I}_1^{\mathcal{E}} &= -[-V_1^{\mathcal{N}} + V_2^{\mathcal{N}}] - R_1^{\mathcal{E}} I_1^{\mathcal{E}} \\
L_2^{\mathcal{E}} \dot{I}_2^{\mathcal{E}} &= -[-V_2^{\mathcal{N}} + V_3^{\mathcal{N}}] - R_2^{\mathcal{E}} I_2^{\mathcal{E}} \\
L_3^{\mathcal{E}} \dot{I}_3^{\mathcal{E}} &= -[-V_3^{\mathcal{N}} + V_4^{\mathcal{N}}] - R_3^{\mathcal{E}} I_3^{\mathcal{E}} \\
L_4^{\mathcal{E}} \dot{I}_4^{\mathcal{E}} &= -[-V_1^{\mathcal{N}} + V_4^{\mathcal{N}}] - R_4^{\mathcal{E}} I_4^{\mathcal{E}} \\
L_5^{\mathcal{E}} \dot{I}_5^{\mathcal{E}} &= -[V_1^{\mathcal{N}} - V_3^{\mathcal{N}}] - R_5^{\mathcal{E}} I_5^{\mathcal{E}}
\end{aligned}$$

Equation 1.5 represent the induced current of the capacitor connected in parallel to the associated load. KCL is used on the configurations represented in the middle of Figure 1.1 connecting the capacitor, generator current and transmission line current. The induced currents are then expressed below where all the parameters are previously defined.

$$\mathcal{C}_k^{\mathcal{N}} \dot{V}_k^{\mathcal{N}} = \sum_j b_{kj}^{\mathcal{E}} I_j^{\mathcal{E}} + \sum_i b_{ki}^{\mathcal{G}} I_k^L$$

For the case specific MG the capacitor currents are defined as the set of the four equations below, representing the characteristics of the four capacitors coupled in parallel with the ZI-loads.

$$\begin{aligned}
\mathcal{C}_1^{\mathcal{N}} \dot{V}_1^{\mathcal{N}} &= [-I_1^{\mathcal{E}} - I_4^{\mathcal{E}} + I_5^{\mathcal{E}}] + [I_1^{\mathcal{G}}] - I_1^L \\
\mathcal{C}_2^{\mathcal{N}} \dot{V}_2^{\mathcal{N}} &= [I_1^{\mathcal{E}} - I_2^{\mathcal{E}}] + [I_2^{\mathcal{G}}] - I_2^L \\
\mathcal{C}_3^{\mathcal{N}} \dot{V}_3^{\mathcal{N}} &= [I_2^{\mathcal{E}} + I_c^{\mathcal{E}} - I_5^{\mathcal{E}}] + [I_3^{\mathcal{G}}] - I_3^L \\
\mathcal{C}_4^{\mathcal{N}} \dot{V}_4^{\mathcal{N}} &= [-I_3^{\mathcal{E}} + I_4^{\mathcal{E}}] + [I_4^{\mathcal{G}}] - I_4^L
\end{aligned}$$

Equation 1.6 and 1.7 are already explained as the power consumption in the loads and the voltage regulation of the DGs, when so far disregarding the outer loop controller $u_{tot}$.

## 1.2 Energy Modelling of Electrical Network: A Port-Hamiltonian Approach

In the associated specialization project the direct current microgrid was modelled with the *input - state - output* port Hamiltonian (pH) formalism. The pH formalism is a mathematical description used to rewrite

the differential equations of the system dynamics with matrix notation [9]. Moreover, it is used to simplify the modelling of the electrical network while underscoring the system energy and emphasizing the system interconnection patterns and energy dissipation matrices. This formalism also provides a useful starting point for finding a Lyapunov function. In turn, Lyapunov functions are a very useful tool when analysing the stability of nonlinear systems. The Lyapunov stability criteria may also be applicable for the linear systems even though other stability criteria as e.g. eigenvalue analysis may also be applied. In this thesis, the Lyapunov stability theory is chosen as the primary stability criteria in order to facilitate using the proofs on other linear and nonlinear systems in further studies. In addition, *Part B* and *Part C* of this thesis study how to design stable and robust controllers against cyber attacks where one of the most effective techniques is based on Lyapunov's theory bounding the stability of the system with respect to the attacks.

For power networks (such as MGs) there are three main advantages of using the pH description. The first advantage is the *port-based* modelling capability, providing a unified framework for modelling interconnections between different physical domains e.g. mechanical, electrical, thermal etc. or different sub-systems within the same domain. The port-based modelling is a graphical notation emphasizing the structure of the physical system as a collection of ideal components linked by edges, preserving the interconnected energy flows. The ideal components are in this sense defined as components that are able to capture the real physical characteristics in each domain [9]. This port-based modelling is very useful in this study where the ports are necessary both when establishing the interconnections between the three electrical sub-systems: i.e., when the two graphs are connected and when interconnecting the final CP MG. In addition, the port-based property is very useful when the electrical network is interconnected with the distributed control network constituting a combined cyber-physical domain.

The second advantage of using the pH formalism is its *geometric properties*. The dynamics of the model are represented in a coordinate-free manner using state space description with a Hamiltonian function representing the stored energy of the system. This simplifies the stability analyses of complicated dynamical systems as the geometric properties emphasize the intrinsic features such as symmetry and conserved quantities in a transparent way [9].

The final advantage of using the pH formalism is the *system and control* property emphasizing that the system is open to interaction through input-ports and output-ports and thereby susceptible to control interactions [9]. This property is used when the dynamics of the final PI-controller in the distributed control network are to be designed from the passivity based techniques later explained in Section 3.

The final *input-state-output* pH model is presented in 1.8 with *port* variables defined as the input and output vectors of the interconnected domains; physical and cyber.

$$\sum_{u,y} \begin{cases} \dot{\mathbf{x}} = \mathbf{F}\boldsymbol{\nabla} H(x) + \mathbf{g}\mathbf{u} + \mathbf{E} & \mathbf{F} \triangleq [\mathbf{J}(\mathbf{x}) - \mathbf{R}(\mathbf{x})] \\ \mathbf{y} = \mathbf{g}^\top(\mathbf{x})\boldsymbol{\nabla} H(x) & H(x) = \frac{1}{2}\mathbf{x}^\top \mathbf{Q}\mathbf{x} \end{cases} \tag{1.8}$$

$\mathbf{x}$ is the state space vector $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{u}$ is the control action, $\mathbf{u} \in \mathbb{R}^m$, where $m \leq n$. $H(x)$ is the Hamiltonian: i.e., the function describing the stored energy of the system. It is a scalar and has the property of $H(x) > 0$.The $\mathbf{J}$ matrix is the natural interconnection matrix containing all the connections related to power preservation. Hence, the $\mathbf{J}$ matrix is skew symmetric, that is $\mathbf{J} = -\mathbf{J}^\top$. $\mathbf{R}$ is the dissipation matrix representing the damping of the system. It has the property of being positive semi definite and symmetric, $\mathbf{R} = \mathbf{R}^\top \geq 0$ [10].

In order to present the interconnected electrical network as a pH system, all the DGs, TLs and loads need to admit the pH formalism. This pH modelling approach is presented below, and the final input-to-state pH representation of the electrical system is subsequently modelled.

**pH model of the DGs**

In order to obtain the *input-state-output* pH representation of of all the generators, all the necessary matrices are first defined. $\mathbf{x}^{\mathcal{G}} = \text{col}(\phi_i^{\mathcal{G}}) \in \mathbb{R}^4$ represents a collection of the energy variables defined as magnetic flux linkages of the generators. $\mathbf{J}^{\mathcal{G}}$ contains the interconnections between the DGs and are defined as a $(4 \times 4)$ zero-matrix as the DGs are not directly interconnected due to the topology of Graph 1. $\mathbf{R}^{\mathcal{G}} = \text{diag}(R_i^{\mathcal{G}} + R_i^{\mathcal{D}}) \in \mathbb{R}^{4\times4}$ contains all the dissipation within each DG. $\mathbf{Q}^{\mathcal{G}} = \text{diag}(L_i^{-1}) \in \mathbb{R}^{4\times4}$ is the quadratic matrix used to describe the geometric properties of the pH model, and the relationship between the change in stored energy and the states is then expressed as: $\mathbf{Q}^{\mathcal{G}}\mathbf{X}^{\mathcal{G}} = \text{col}(\frac{\phi_i}{L_i}) = \text{col}(I_i^{\mathcal{G}}) = \boldsymbol{\nabla} H^{\mathcal{G}}(x^{\mathcal{G}}) \in \mathbb{R}^4$. The two entering matrices, $\mathbf{g}_p^{\mathcal{G}} = \mathbf{g}_i^{\mathcal{G}} = \mathcal{I} \in \mathbb{R}^{4\times4}$, describes where the port variables are entering the DGs and the associated $\mathbf{u}_p^{\mathcal{G}}$, $\mathbf{u}_{tot}^{\mathcal{G}}$ matrices represents the actual input port variables: $\mathbf{u}_p^{\mathcal{G}} = \text{col}(u_{pi}^{\mathcal{G}}) \in \mathbb{R}^4$ $\mathbf{u}_{tot}^{\mathcal{G}} = \text{col}(u_{tot,i}^{\mathcal{G}}) \in \mathbb{R}^4$. The port variables are unknown until the generators are interconnected with another sub-system, also admitting the pH formalism. $\mathbf{E}^{\mathcal{G}} = \text{col}(V_{nom}) \in \mathbb{R}^4$ contains the constant voltage sources in the generators. The final pH model

of the DGs are then obtained and presented below by using the formalism given in 1.8, when the Hamiltonian is defined as $H(x^{\mathcal{G}}) = \frac{1}{2}\mathbf{x}^{\mathcal{G}\top}\mathbf{Q}^{\mathcal{G}}\mathbf{x}^{\mathcal{G}}$.

$$\sum_{\text{DGs}} : \begin{cases} \dot{\mathbf{x}}^{\mathcal{G}} = (-\mathbf{R}^{\mathcal{G}})\boldsymbol{\nabla} H(x^{\mathcal{G}}) + \mathbf{g}_p^{\mathcal{G}}\mathbf{u}_p^{\mathcal{G}} + \mathbf{g}_{tot}^{\mathcal{G}}\mathbf{u}_{tot}^{\mathcal{G}} + \mathbf{E}^{\mathcal{G}} \\ \mathbf{y}_p^{\mathcal{G}} = \mathbf{g}_p^{\mathcal{G}\top}\boldsymbol{\nabla} H(x^{\mathcal{G}}) \\ \mathbf{y}_{tot}^{\mathcal{G}} = \mathbf{g}_i^{\mathcal{G}\top}\boldsymbol{\nabla} H(x^{\mathcal{G}}) \end{cases} \tag{1.9}$$

**pH model of the transmission lines**

In order to obtain the *input-state-output* PH representation of of all the transmission lines, all the necessary matrices are first defined. $\mathbf{x}^{\mathcal{E}} = \text{col}(\phi_j^{\mathcal{E}}) \in \mathbb{R}^5$ represents a collection of energy variables defined as the magnetic flux linkages of the TLs. $\mathbf{J}^{\mathcal{G}}$ contains the interconnections between the TLs and are defined as a $(5 \times 5)$ zero-matrix as the TLs are not directly interconnected due to the topology of Graph 2. $\mathbf{R}^{\mathcal{E}} = \text{diag}(R_j^{\mathcal{E}}) \in \mathbb{R}^{5\times5}$ contains all the dissipation of the TLs. $\mathbf{Q}^{\mathcal{E}} = \text{diag}(L_j^{-1}) \in \mathbb{R}^{5\times5}$ is the quadratic matrix used to describe the geometric properties of the pH model and the relationship between the change in stored energy and the states is then expressed as: $\mathbf{Q}^{\mathcal{E}}\mathbf{X}^{\mathcal{E}} = \text{col}(\frac{\phi_j}{L_j}) = \text{col}(I_j^{\mathcal{E}}) = \boldsymbol{\nabla} H^{\mathcal{E}}(x^{\mathcal{E}}) \in \mathbb{R}^5$. The entering matrix, $\mathbf{g}_p^{\mathcal{E}} = \mathcal{B}^{\mathcal{E}\top}$, equals the transposed incidence matrix of Graph 2 and the associated $\mathbf{u}_p^{\mathcal{E}}$ matrix represents the actual input port variables: $\mathbf{u}_p^{\mathcal{E}} = \text{col}(u_{pj}^{\mathcal{E}}) \in \mathbb{R}^5$. The port variables are unknown until the TLs are interconnected with another sub-system, also admitting the pH formalism. $\mathbf{E}^{\mathcal{E}}$ is a zero-column matrix as the TL are passive components with no constant sources. The final pH model of the TLs are then obtained and presented below by using the formalism given in 1.8, when the Hamiltonian is defined as $H(x^{\mathcal{E}}) = \frac{1}{2}\mathbf{x}^{\mathcal{E}\top}\mathbf{Q}^{\mathcal{E}}\mathbf{x}^{\mathcal{E}}$.

$$\sum_{\text{TLs}} : \begin{cases} \dot{\mathbf{x}}^{\mathcal{E}} = (-\mathbf{R}^{\mathcal{E}})\boldsymbol{\nabla} H(x^{\mathcal{E}}) + \mathbf{g}_p^{\mathcal{E}}\mathbf{u}_p^{\mathcal{E}} \\ \mathbf{y}_p^{\mathcal{E}} = \mathbf{g}_p^{\mathcal{E}\top}\boldsymbol{\nabla} H(x^{\mathcal{E}}) \end{cases} \tag{1.10}$$

**pH model of the loads**

In order to obtain the *input-state-output* PH representation of of all the loads, all the necessary matrices are first defined. $\mathbf{x}^{\mathcal{N}} = \text{col}(q_k^{\mathcal{N}}) \in \mathbb{R}^4$ represents a collection of energy variables defined as the electrical charges. $\mathbf{J}^{\mathcal{N}}$ contains the interconnections between the loads defined as a $(4\times4)$ zero-matrix as the loads are not directly interconnected due to the topology of both Graph 1 and 2. $\mathbf{G}_{cte}^{\mathcal{N}} = \text{diag}(G_k^{\mathcal{N}}) \in \mathbb{R}^{4\times4}$ contains the dissipation of the loads. $\mathbf{Q}^{\mathcal{N}} = \text{diag}(C_k^{-1}) \in \mathbb{R}^{4\times4}$ is the quadratic matrix used to describe the geometric properties of the pH model and the relationship between the change in stored energy and the states is then expressed as: $\mathbf{Q}^{\mathcal{N}}\mathbf{X}^{\mathcal{N}} = \text{col}(\frac{q_k}{C_k}) = \text{col}(V_k^{\mathcal{N}}) = \boldsymbol{\nabla} H^{\mathcal{N}}(x^{\mathcal{N}}) \in \mathbb{R}^4$. The two entering matrices, $\mathbf{g}_{p1}^{\mathcal{N}} = \mathbf{g}_{p2}^{\mathcal{N}} = \mathcal{I} \in \mathbb{R}^4$, describes where the port variables are entering the loads and the associated $\mathbf{u}_{p1}^{\mathcal{N}}$, $\mathbf{u}_{p2}^{\mathcal{N}}$ matrices represents the actual input port variables: $\mathbf{u}_{p1}^{\mathcal{N}} = \text{col}(u_{p1,k}^{\mathcal{N}}) \in \mathbb{R}^4$ $\mathbf{u}_{p2}^{\mathcal{N}} = \text{col}(u_{p2,k}^{\mathcal{N}}) \in \mathbb{R}^4$. The port variables are unknown until the loads are interconnected with other sub-systems, also admitting the pH formalism. $\mathbf{E}^{\mathcal{N}} = \text{col}(I_k^{cte}) \in \mathbb{R}^4$ contains the constant current sources in the ZI-loads. The final pH model of the loads are then obtained and presented below by using the formalism given in 1.8, when the Hamiltonian is defined as $H(x^{\mathcal{N}}) = \frac{1}{2}\mathbf{x}^{\mathcal{N}\top}\mathbf{Q}^{\mathcal{N}}\mathbf{x}^{\mathcal{N}}$.

$$\sum_{\text{Loads}} : \begin{cases} \dot{\mathbf{x}}^{\mathcal{N}} = (-\mathbf{G}_{cte}^{\mathcal{N}})\boldsymbol{\nabla} H(x^{\mathcal{N}}) + \mathbf{g}_{p1}^{\mathcal{N}}\mathbf{u}_{p1}^{\mathcal{N}} + \mathbf{g}_{p2}^{\mathcal{N}}\mathbf{u}_{p2}^{\mathcal{N}} + \mathbf{E}^{\mathcal{N}} \\ \mathbf{y}_{p1}^{\mathcal{N}} = \mathbf{g}_{p1}^{\mathcal{N}\top}\boldsymbol{\nabla} H(x^{\mathcal{N}}) \\ \mathbf{y}_{p2}^{\mathcal{N}} = \mathbf{g}_{p2}^{\mathcal{N}\top}\boldsymbol{\nabla} H(x^{\mathcal{N}}) \end{cases} \tag{1.11}$$

## 1.3 Energy Modelling of Interconnected Physical Network

The three sub-systems are now shown to admit the pH formalism and the systems are interconnected, establishing one final electrical network expressed as pH model of the physical layer. Graphs 1 and 2 are used to interconnect the electrical network where the generators are connected to the loads through the generator edges defined in Graph 1, and the loads are interconnected through the transmission lines defined in Graph 2. This is presented below in Figure 1.4.

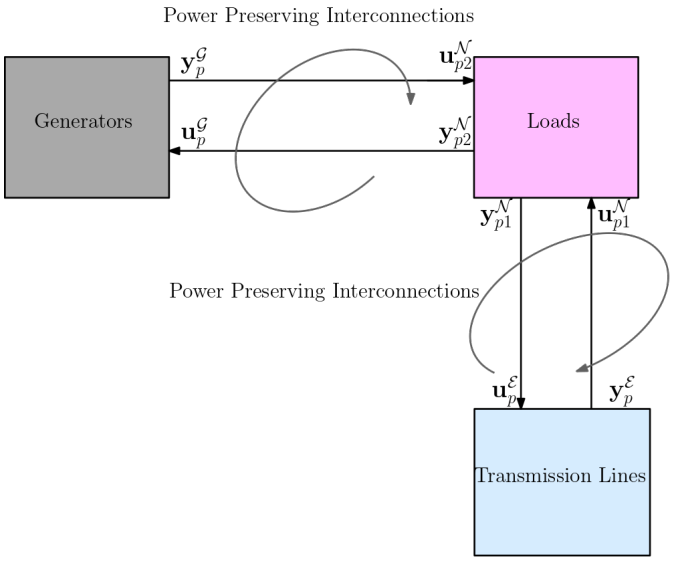


Figure 1.4: pH representation of the electrical interconnected system

The *geometric properties* are defined as skew-symmetric relations between the input and output *port variables* of the sub-systems. Power preservation is therefore ensured when the input and output values of the individual systems are cancelling out, due to the dynamics presented in 1.1.2 combined with the skew-symmetric properties. The skew-symmetric interconnections presented in Figure 1.4 are then presented with matrix notation below.

$$\begin{bmatrix} \mathbf{u}_p^{\mathcal{G}} \\ \mathbf{y}_p^{\mathcal{G}} \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{u}_{p2}^{\mathcal{N}} \\ \mathbf{y}_{p2}^{\mathcal{N}} \end{bmatrix} \qquad \begin{bmatrix} \mathbf{u}_p^{\mathcal{E}} \\ \mathbf{y}_p^{\mathcal{E}} \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{u}_{p1}^{\mathcal{N}} \\ \mathbf{y}_{p1}^{\mathcal{N}} \end{bmatrix} \tag{1.12}$$

The completed electrical network is presented below, using the formalism defined in 1.8 combined with the skew-symmetric power preserving interconnections between the three pH sub-systems.

$$\sum_{tot} : \begin{cases} \dot{\mathbf{x}}_{tot} = (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(x_{tot}) + \mathbf{g}_i^{\mathcal{G}} \mathbf{u}_{tot} + \mathbf{E}_{tot} \\ \mathbf{y}_{tot} = \mathbf{g}_i^{\mathcal{G}\top} \boldsymbol{\nabla} H_{tot}(x_{tot}) \end{cases} \tag{1.13}$$

$\mathbf{x}_{tot} = \text{col}(x_{tot}) \in \mathbf{R}^{(n^{\mathcal{G}}+n^{\mathcal{E}}+n^{\mathcal{N}})}$ represents the electrical energy state vector containing all the flux linkages of the DGs, flux linkages of the TLs and electrical charges of the loads. For the case specific MG the energy state vector will have the dimension $\mathbb{R}^{12}$. $\mathbf{J}_{tot} = \begin{bmatrix} 0 & 0 & -\mathcal{B}^{\mathcal{G}\top} \\ 0 & 0 & -\mathcal{B}^{\mathcal{E}\top} \\ \mathcal{B}^{\mathcal{G}} & \mathcal{B}^{\mathcal{E}} & 0 \end{bmatrix} \in \mathbb{R}^{12\times 12}$ is the interconnection matrix, containing both of the two incidence matrices of Graph 1 and 2. The inherent block-matrices have dimensions $\mathcal{B}^{\mathcal{G}} \in \mathbb{R}^{4\times 4}$ and $\mathcal{B}^{\mathcal{G}} \in \mathbb{R}^{4\times 5}$ giving the final dimension of $(12 \times 12)$ and the block matrix dimension $(3 \times 3)$. $\mathbf{R}_{tot} = \text{diag}((\mathbf{R}^{\mathcal{G}} + \mathbf{R}^{D}), \mathbf{R}^{\mathcal{E}}, \mathbf{G}^{\mathcal{N}}) \in \mathbb{R}^{12\times 12}$ contains all the electrical dissipation. $\mathbf{g}_i^{\mathcal{G}} \in \mathbb{R}^{12}$ is the input matrix of the DGs not yet canceled out due to any power preserving interconnections. Equally $\mathbf{u}_{tot} \in \mathbb{R}^{12}$ is still a control input matrix entering the DGs. This introduces a passive output of the electrical network, $\mathbf{y}_{tot} \in \mathbb{R}^{12}$, facilitating interconnections to an outer loop control system with a controller modelled based on passivity. This is later carried out when the final cyber-physical MG is modelled. $\mathbf{E}_{tot} = \text{col}(\mathbf{V}_{nom}, \mathbf{0}, \mathbf{I}^{cte}) \in \mathbb{R}^{12} : \mathbf{V}_{nom} \in \mathbb{R}^4, \mathbf{0} \in \mathbb{R}^5, \mathbf{I}^{cte} \in \mathbb{R}^4$ contains all the constant sources of the electrical network. *Appendix* D include an overview of the Lyapunov stability proof of the droop controlled electrical network, conducted in the associated specialization project. The proof concludes that the decentralized primary droop controller is able to ensure sub-optimal operations of the MG by limiting the voltage deviations and ensuring steady state stability when inherent system changes occur. The primary controller ensures that the electrical power system asymptotically converges to the minimum equilibrium achieving stable operations. However, the controller is not able to restore any initial conditions when different system changes appears. The DC MG controller is therefore further modelled, aiming to optimize the operations of the power system.

# 2 Model of the Distributed Control Network

A secondary PI-controller is therefore implemented as an outer loop controller given the task of restoring operating conditions of the MG to the desired optimal steady-state. Towards this end, the control network is

modelled as a cyber network: i.e., the physical units of the electrical system are, in addition, interconnected through communication links in a cyber layer. The controller is designed using *control by interconnection*(CbI) philosophy; i.e., by interconnecting the distributed cyber control network (admitting a pH representation) with the rest of the physical system through a lossy interconnection pattern, whose virtual dissipation is the proportional term of the PI. The generating units cooperatively decide the operational states of each DG with the ambition of steering the MG to the optimal steady state where the desired control objectives are satisfied. In order to ensure this optimal operations, the control objectives needs to be established so that the secondary controller subsequently may be modelled as the final element ensuring optimal operations of the cyber-physical MG.

## 2.1 Control Objectives

The control objectives are implemented as the optimal operating conditions of the MG. The optimal operations are defined as the point where the MG achieves *proportional current-sharing* and *average voltage regulation* here referred to as control objective *1* and *2* respectively. Current-sharing allows the DGs to proportionally share their generation capacity, preventing over-stress in the distributed units and facilitating safe and stable operations of the network [8]. In 1.3 it is presented that the currents depend on the voltage differences and not an absolute value of the load voltages. Due to this modulation, the optimal value of the proportionally shared capacity may be satisfied for many voltage levels. The second control objective is then to regulate the average voltage across the whole microgrid towards an average voltage reference equal to the nominal voltage [1]. The stability of the voltage within the system will be of critical influence when the MG is operating in islanded mode. Voltage regulation is therefore required to ensure the proper functioning of the connected loads operating within specified power limits [1].

The conditions necessary to ensure the first control objective, are obtained by solving the economic dispatch problem with the Lagrangian dual problem formulation solved with the Karush-Kuhn-Tucker (KKT) conditions. The economic dispatch formulation is presented below as a primal optimization problem, where the objective function represents the sum of the DG's cost functions, $C_i(I_i^{\mathcal{G}}) = \alpha_i(I_i^{\mathcal{G}})^2 + \beta_i(I_i^{\mathcal{G}}) + \gamma_i, \quad \forall i \in \mathcal{G}$. $\alpha$, $\beta$ and $\gamma$ are parameter values describing the weightings of each DG with respect to the cost of generation [1].

$$\begin{aligned} \underset{i^{\mathcal{G}}}{\text{Minimize}} \quad & \sum_{i\in\mathcal{G}} C_i(I_i^{\mathcal{G}}) \\ \text{subject to} \quad & \sum_{i\in\mathcal{G}} (I_i^{\mathcal{G}}) = I_{\text{Demand}} \quad \forall i \in \mathcal{G} \end{aligned} \tag{2.1}$$

The Lagrangian dual problem formulation is then used to redefine the problem so that the KKT conditions may be used to obtain the optimal solution. The idea behind Lagrangian duality is to take the constraints into account by arguing the objective function as a weighted sum of the constraints. Formally the Lagrangian function is formulated as $L(x, \eta, \lambda) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{j=1}^{p} \lambda_j g_j(x)$ [11]. The problem formulation in 2.1 the associated Lagrangian dual problem is expressed as:

$$\begin{aligned} L(I_i^{\mathcal{G}}, \lambda) &= f(I_i^{\mathcal{G}}) + \lambda g(I_i^{\mathcal{G}}) \\ &= \sum_{i\in\mathcal{G}} C_i(I_i^{\mathcal{G}}) + \lambda(I_{\text{Demand}} - \sum_{i\in\mathcal{G}} I_i^{\mathcal{G}}) \end{aligned} \tag{2.2}$$

$\lambda$ is the incremental costs of the DGs also defined as the dual variables or Lagrangian multiplier in the sense of convex optimization theory. The Lagrangian multiplier represents the change in the objective function, $f_0(x, \lambda)$ when changing the equality constraint, $g(x)$, with one incremental unit, $\lambda = \frac{\Delta f}{\Delta g}$ [11]. In this analysis, the Lagrangian multipliers are interpreted as the incremental costs of each DG, representing the changes in the DGs cost functions when the total demand of the MG, $I_{\text{Demand}}$, changes.

The objective function in 2.1 is convex and the problem formulation is, therefore, a convex optimization problem. Hence, the optimal value is a global optimum as well as a local optimum[11]. Since the primal optimization is a convex problem and Slater's condition is satisfied, the KKT conditions are used to obtain *primal* and *stationary conditions* for the optimal solution in the network. The stationary conditions are first

assessed below, derived from KKT conditions.

Stationary conditions: (2.3)

$$\frac{dL}{dI_i^{\mathcal{G}}} \rightarrow \begin{cases} \frac{dL}{dI_1^{\mathcal{G}}} = 2\alpha_1 I_1^{\mathcal{G}} + \beta_1 - \lambda \\ \frac{dL}{dI_2^{\mathcal{G}}} = 2\alpha_2 I_2^{\mathcal{G}} + \beta_2 - \lambda \\ \frac{dL}{dI_3^{\mathcal{G}}} = 2\alpha_3 I_3^{\mathcal{G}} + \beta_3 - \lambda \\ \frac{dL}{dI_4^{\mathcal{G}}} = 2\alpha_4 I_4^{\mathcal{G}} + \beta_4 - \lambda \end{cases} \qquad \frac{dL}{dI_i^{\mathcal{G}}} = 0 \rightarrow \begin{cases} \lambda = 2\alpha_1 I_1^{\mathcal{G}} + \beta_1 \\ \lambda = 2\alpha_2 I_2^{\mathcal{G}} + \beta_2 \\ \lambda = 2\alpha_3 I_3^{\mathcal{G}} + \beta_3 \\ \lambda = 2\alpha_4 I_4^{\mathcal{G}} + \beta_4 \end{cases}$$

Control objective *1* is then presented as the solution of the stationary conditions, defined as *equal incremental cost* criteria [12]. This criterion ensures that the costs of generation are dispatched economically between the DGs, where the cost of delivering one additional increment of power is equal for all generating units [12]. Hence, the equal incremental cost, when $t \rightarrow \infty$ and all the generators achieve the same equal incremental cost, is defined as the optimal cost of generation $\lambda_{opt}$[1]. The control objective *1* is formally defined below where $\lambda_i$ and $\lambda_j$ are the neighbouring connected nodes.

$$\textbf{Control Objective 1:} \quad \lim_{t\rightarrow\infty} (\lambda_i = \lambda_j = \lambda_{opt}) \tag{2.4}$$

The second control objective is defined in 2.5, with the goal of ensuring that the sum of the weighted DG voltages is as close to the pre-defined nominal network voltage as possible. This control objective is accounted by adding weightings, $\mathbf{w}^{-1}$, in the interconnections between the control network and the electrical network: i.e., in the CP pH interconnections later carried out in Section 2.5.

$$\textbf{Control Objective 2:} \quad \lim_{t\rightarrow\infty} \sum_{i\in\mathcal{G}} \omega_i V_i = V_{nom} \sum_{i\in\mathcal{G}} \omega_i, \qquad \omega_i > 0, \forall i \in \mathcal{G} \tag{2.5}$$

Hence, the second control objective regulates the weighted average voltage across the whole microgrid towards the nominal voltage value of the system. This is desirable as the current output of each generator: i.e., the port variable outputs of the electrical network, depends on the voltage differences of the connected DGs and not an absolute value of a bus voltage. This is due to the model of the droop controller, limiting the voltage deviations by regulating the DG's currents.

## 2.2 Control Network Modelling Using Graph Theory

When proposing the dynamics of the secondary controller, incorporating both droop control and cyber control, the first step is to design the distributed control network dynamics. When the distributed network is modelled, the same graph theory – as presented for the electrical network – is applied. The additional *Graph 3* is established, with inherent dynamics based on the *consensus protocol*. Hence, the distributed control network constitutes the cyber layer. This section aims to design a pH system representation of the cyber layer subsequently connected with the pH system of the physical layer, assembling the cyber-physical MG.

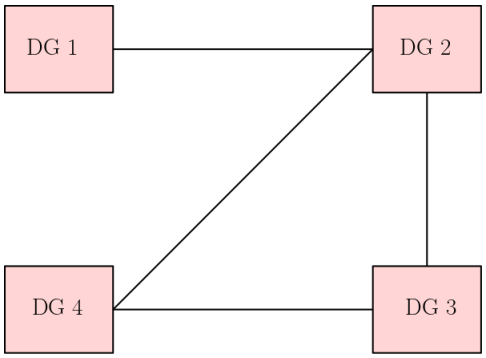


Figure 2.1: Graph 3

*Graph 3:* $\mathcal{M}_c = (\mathcal{N}_c, \mathcal{E}_c, \mathcal{A})$ in Figure 2.1 is the undirected and unbalanced graph representing the four distributed generators and communication links between an arbitrary choice of communicating units. $\mathcal{N}_c$ is the set of nodes: i.e., set of DGs, $\mathcal{E}_c$ is the set of edges: i.e., set of communication links and $\mathcal{A}$ is the *Adjacency* matrix. As previously mentioned in Section 1.1.1 the Adjacency matrix, together with the *Degree* matrix and

the *Laplacian*, are necessary matrices when modelling and assessing a network with communicating units. The Adjacency matrix, $\mathcal{A}$, defines the connecting nodes to the node of study: i.e., defining which nodes that are the neighbouring nodes of the vertex object. The $\mathcal{A}$-matrix is obtained without taking into account the direction of flow between the communicating units. The matrix only attributes real and positive numbers where element $a_{ij}$ equals 1 if node $i$ and node $j$ are connected, otherwise $a_{ij}$ equals 0. The Adjacency matrix has the property of being symmetric where $\mathcal{A} = \mathcal{A}^T$ with the dimension of $\{n_{\mathcal{M}_c}^{\mathcal{N}_c} \times n_{\mathcal{M}_c}^{\mathcal{N}_c}\}$. The $\mathcal{A}$-matrix of the communication Graph 3 for the case specific MG is then given as:

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \tag{2.6}$$

The *Degree* matrix, $\mathcal{D}$, is a symmetric diagonal matrix with the dimension $\{m_{\mathcal{M}_c}^{\mathcal{E}_c} \times m_{\mathcal{M}_c}^{\mathcal{E}_c}\}$ where $\mathcal{D} = \mathcal{D}^\top$. The diagonal elements equals the sum of the nodes connected to the vertex objects: i.e., the summation of each row in the adjacency matrix for each vertex object, defined as $d_{ii} = \sum_{j=1}^{n} a_{ij}$. Hence, the matrix contains the information on how many edges each node receives. The $\mathcal{D}$-matrix of the communication Graph 3 for the case specific MG is then given as:

$$\mathcal{D} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \tag{2.7}$$

The *Laplacian* matrix $\mathcal{L}$, can arguably be viewed as the most important matrix in regards to assessing the stability of systems with communication networks. The $\mathcal{L}$-matrix contains the consensus properties of the communication links, where all variables that mathematically follow the Laplacian are defined as the communicated (data) packages. The matrix is defined as the subtraction of the Degree matrix and Adjacency matrix, $\mathcal{L} \triangleq \mathcal{D} - \mathcal{A}$, $\mathcal{L} \in \{n_G^{\mathcal{N}} \times n_G^{\mathcal{N}}\}$. The Laplacian of the communication Graph 3 for the case specific MG is then presented as:

$$\mathcal{L} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{bmatrix} \tag{2.8}$$

## 2.3 Dynamics of Control Network

The inherent dynamics within the distributed control network: i.e., the cyber control dynamics, are designed with the consensus-based algorithm presented in the associated specialization project and in *Appendix* E for the reader of this thesis. A distributed consensus-based cyber controller is then implemented as in 2.9. $K_i^I > 0$ is the integrator gain controlling the speed of the communication whereas $u_i^c$ is the cyber controller, representing the data shared from generator $i$ to generator $j$. $(u_j^c - u_i^c)$ is the neighbouring error that the controller needs to minimize in order to satisfy control objective *1*, where all incremental costs are equal. This will again ensure proper current-sharing in the network as the incremental costs are a variable depending on the generator current. This is later explained when the electrical network and control network are interconnected giving the relations: $\mathbf{y}_{tot} = \mathbf{u}_c = \mathbf{I}^{\mathcal{G}}$. Hence, the communicated values depends of the DGs currents and associated dynamics constituting the incremental costs of the DGs. The cyber states are defined below and expressed for the case specific MG as the neighbouring error defined by the Adjacency matrix given in 2.6.

$$\dot{x}_c = K_i^I \sum_{j \in N_c} a_{ij}(u_j^c - u_i^c) \quad \longrightarrow \quad \begin{cases} \dot{x}_1 = K_1^I[(u_2 - u_1)] \\ \dot{x}_2 = K_2^I[(u_1 - u_2) + (u_3 - u_2) + (u_4 - u_2)] \\ \dot{x}_3 = K_3^I[(u_2 - u_3) + (u_3 - u_3)] \\ \dot{x}_4 = K_4^I[(u_2 - u_4) + (u_3 - u_4)] \end{cases} \tag{2.9}$$

## 2.4 Energy Modelling of Control Network: A Port-Hamiltonian Approach

The port Hamiltonian formalism is then used to express the open loop model of the cyber layer. Communication Graph 3 combined with the consensus protocol constitutes the distributed control network, as explained in

detail in the specialization project. The final *input-state-output* pH model is also conducted and is presented in 2.10 for the sake of completeness.

In order to facilitate interconnecting the control network with the electrical network, the control network also needs to admit the pH formalism. In addition, the control network needs to have a passive output – equally as the electrical network has a passive output – with respect to the DGs. The two networks can then be interconnected through the passive input/output variables and the final cyber-physical MG achieves power preservation. The same modelling approach is used to obtain the pH model of the control network, as previously presented for the generators, transmission lines and loads. $\mathbf{x}_c = \text{col}(x_i^c) \in \mathbb{R}^4$ contains the cyber energy states of the control network and the interconnection matrix $\mathbf{J}^c \in \mathbb{R}^{4\times4}$ contains the physical interconnections between the DGs in the cyber layer. As the DGs are only connected through the communication links in the control network, the interconnection matrix will only consist of zeroes. There is no dissipation in the control dynamics given in 2.9 and the dissipation matrix $\mathbf{R}^c \in \mathbb{R}^{4\times4}$ will also only contain zeroes. The geometric description is defined by the $\mathbf{K}_I = \mathbf{Q}_c = \text{diag}(K_{I,i}^{-1}) \in \mathbb{R}^{4\times4}$ containing the integral gains of the PI controllers and $\mathbf{K}_I > 0$. $\mathbf{g}_c = \text{col}(-K_i^I l_{ij}) \in \mathbb{R}^{4\times4}$ contains the information about where the input values are entering and how they are controlled with the integral gain. The locations of the different input values are defined by the Laplacian matrix. Hence, the input values $\mathbf{u}^c = \text{col}(u_i^c) \in \mathbb{R}^4$ are entering the control network in two stages: i.e., as the communicated values received from the DGs when the two networks are interconnected and as the values communicated between the DGs. The port variables are unknown until the control network is interconnected with the electrical network. The final pH model of the control network is then obtained and presented below by using the formalism given in 1.8, when the Hamiltonian is defined as $H_c(x_c) = \frac{1}{2}x^{c\top}\mathbf{K}_I^{-1}x^c$.

$$\sum_c \begin{cases} \dot{\mathbf{x}}_c = \mathbf{g}_c\mathbf{u}_c \\ \mathbf{y}_c = \mathbf{g}_c^\top \boldsymbol{\nabla} H_c(x_c) \end{cases} \tag{2.10}$$

## 2.5 Energy Modelling of Cyber-Physical MG: A Port-Hamiltonian Approach

Both the electrical network and the control network are so far shown to admit the pH formalism, and the overall model of the case specific MG is designed by interconnecting the cyber layer and the physical layer through their respective passive input-output port variables substituting the pre-specified interconnection pattern. The interconnection – which includes the proportional term of the PI-controller as virtual losses – can be viewed as a version of the *control by interconnection* (CbI) technique [10]. The physical interconnection between the two networks is represented in Figure 2.2 where $\mathbf{y}_c$ is defined as the passive output of the cyber layer equal to the secondary control input $\mathbf{u}_{tot}$ of the physical layer with the added properties of the interconnections. Consequently, are the cyber controller $\mathbf{u}_c$ equal to the passive output of the physical layer $\mathbf{y}_{tot}$ with the added properties of the associated interconnections.

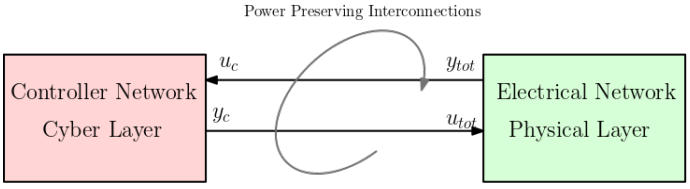


Figure 2.2: pH representation of closed loop control system

The final closed loop control system formed with the CbI technique is then expressed below.

$$\sum_T : \left\{ \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} = \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^\top & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} \right. \tag{2.11}$$

$\mathbf{w}^{-1}$ represents added weightings in the power preserving interconnections, later explained as an important element in order to ensure voltage regulation of the MG. In addition, power dissipation, $\mathbf{r}$, is added to the interconnections representing the secondary PI-controller and the dissipation of the cyber layer. When the CbI technique is used, $\mathbf{r}$ needs to include the proportional gain, $K_P$, contributing with damping of the secondary control constituting flexibility in regards to the control response. For generality, the power preserving interconnections also include some constants, represented in the $b$-vector containing $b$ and $b_c$. The $b$-vector gives the property of being able to later add constants e.g. power sources, without affecting the system stability.

When the closed loop control system now is established it is possible to present the final state space model of the interconnected network as presented below, based on the pH formalism:

$$\dot{\mathbf{x}}_T = (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(x_{tot}) + \mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} + \mathbf{E}_{tot} + \mathbf{g}_c\mathbf{u}_c \tag{2.12}$$

$\mathbf{x}_T = \text{col}(\mathbf{x}_{tot}, \mathbf{x}_c) \in \mathbb{R}^{(n^{\mathcal{G}}+n^{\mathcal{E}}+n^{\mathcal{N}}+n^c)}$ is a collection of all state vectors in the cyber-physical MG. For the case specific MG $\mathbf{x}_T \in \mathbb{R}^{17}$.

The secondary controller is now modelled, aiming to ensure the two control objectives simultaneously at the equilibrium point of the closed loop system. As the closed loop CP MG now is modelled, it is assumed that the final interconnected MG, $\sum_T$, has a unique equilibrium point as both of the sub-networks are modelled with individual equilibrium points, presented pH network representations in 1.13 and 2.10. The first assumption necessary when further implementing the secondary controller, $\mathbf{u}_{tot}$, is then defined below.

**Assumption: 1.** *Given that $\sum_{tot}$ and $\sum_c$ have unique equilibrium points, it is assumed that $\sum_T$ has a unique equilibrium point.*

To summarize: the two passive sub-systems are now interconnected through the input-output port variables: $\mathbf{u}_{tot}, \mathbf{y}_{tot}, \mathbf{u}_c,$ and $\mathbf{y}_c$, resulting in one cyber-physical MG of closed loop expressed as a pH system. The distributed control network connects to the electrical network through the DGs as the distributed generators will have additional port-variables after the electrical interconnections are established. When studying the passive output of the electrical network, it is presented that this output equals the output of the distributed generators: i.e., the generated currents. It is then presented that the passive output of the electrical network equals the generated currents of each DG when the MG is of closed loop: $\mathbf{y}_{tot} = \mathbf{u}_c = \mathbf{I}^{\mathcal{G}}$.

### 2.5.1 Energy Flows and Stability of Cyber-Physical MG

The energy flow analysis of the closed loop CP MG and subsequently the steady state stability assessment is presented below in this section. The theoretical approach is explained in detail in the associated specialization project and later in *Part B* Section 5.12. For the sake of completeness of this thesis, the energy flows of the closed loop CP MG are summarized and presented, ensuring the reader that the interconnected MG achieves stable operations at the converged equilibrium.

The total stored energy: i.e., the Hamiltonian of the cyber-physical MG $H_T(x_T)$ is given below, including the virtual energy stored in the integrator state of the PI.

$$H_T(x_T) = H_{tot}(x_{tot}) + H_c(x_c) = \frac{1}{2}\mathbf{x}_{tot}^\top \mathbf{Q}_{tot}\mathbf{x}_{tot} + \frac{1}{2}\mathbf{x}_c^\top \mathbf{K}_I^{-1}\mathbf{x}_c, \tag{2.13}$$

The time-derivative of the total stored energy is then given below as the sum of the time-derivative of the individual sub-systems energy.

$$\begin{aligned}
\dot{H}_T(x_T) &= \dot{H}_{tot}(x_{tot}) + \dot{H}_c(x_c) \\
&= \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{F}_{tot}\boldsymbol{\nabla} H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(H_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c && (2.14)\\
&= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla} H_{tot}(x_{tot}) - \mathbf{y}_{tot}^\top \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_{tot}^\top \mathbf{b} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \mathbf{y}_c^{-1}\mathbf{y}_{tot}\mathbf{w} + \mathbf{y}_c^\top \mathbf{b}_c && (2.15)\\
&= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla} H_{tot}(x_{tot}) + \mathbf{y}_{tot}^\top \mathbf{b} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \mathbf{y}_c^\top \mathbf{b}_c && (2.16)
\end{aligned}$$

We arrive at the final time-dependent energy function due to the power preserving properties presented in the closed loop system in 2.11 where the terms two and four in equation 2.14 can be expressed as:

$$\begin{aligned}
\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} &= \mathbf{y}_{tot}^\top \mathbf{u}_{tot} \\
&= \mathbf{y}_{tot}^\top(-\mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{b}) \\
&= -\mathbf{y}_{tot}^\top \mathbf{r}\mathbf{y}_{tot} - \mathbf{y}_{tot}^\top \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_{tot}^\top \mathbf{b} && (2.17)\\
\boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c &= \mathbf{y}_c^\top \mathbf{u}_c \\
&= \mathbf{y}_c^\top(\mathbf{w}^{-1\top}\mathbf{y}_{tot} + \mathbf{b}_c) \\
&= \mathbf{y}_c^\top \mathbf{w}^{-1\top}\mathbf{y}_{tot} + \mathbf{y}_c^\top \mathbf{b}_c && (2.18)
\end{aligned}$$

Recognizing – in the above representations – that the two terms are cancelling out due to the power preserving interconnections: $\mathbf{y}_c^\top \mathbf{w}^{-1\top} \mathbf{y}_{tot} - \mathbf{y}_{tot}^\top \mathbf{w}^{-1} \mathbf{y}_c = 0$. The dissipation of the PI-controller, $\mathbf{r}$, is added to the closed loop MG's dissipation matrix $\mathbf{T}_T = \text{blockdiag}\{(\mathbf{R}^{\mathcal{G}} + \mathbf{R}^{\mathcal{D}} + \mathbf{r}), \mathbf{R}^{\mathcal{E}}, \mathbf{G}^{\mathcal{N}}\} \geq 0$, $\mathbf{T}_T \in \mathbb{R}^{(3\times3)}$ representing physical dissipation with respect to only the states of the physical network, $\mathbf{x}_{tot}$.

In order to obtain the Lyapunov stability certificate the Lyapunov candidate is proposed based on the above Hamiltonian and incremental energy. Incremental energy is applied in order to ensure that the converged equilibrium is the minimum point of interest. The Lyapunov function presented in 2.19 is therefore expressed with the incremental states $\tilde{\mathbf{x}} = \mathbf{x} - \bar{\mathbf{x}}$, where $\bar{\mathbf{x}}$ represents the states at the minimum equilibrium and $\mathbf{x}$ represents the present operating states. All constants are additionally removed from the function when the system is modelled with incremental energy, as they are cancelled out due to the definition.

$$\begin{aligned} V_T(\tilde{x}_T) &= H_{tot}(\tilde{x}_{tot}) + H_c(\tilde{x}_c) \\ &= \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot} \tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top \mathbf{K}_I \tilde{\mathbf{x}}_c \end{aligned} \tag{2.19}$$

$$\begin{aligned} \dot{V}_T(\tilde{x}_T) &= \dot{H}_{tot}(\tilde{x}_{tot}) + \dot{H}_c(\tilde{x}_c) \\ &= -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot}) \mathbf{T}_T \boldsymbol{\nabla} H_{tot}(\tilde{x}_{tot}) \leq 0 \end{aligned} \tag{2.20}$$

The final Lyapunov stability proof of the closed loop CP MG is presented in *Appendix* D. It concludes that the secondary controller is able to bring the CP MG to steady state operations at an equilibrium certified to be the desired minim operating value. Hence, the closed loop model is proven to ensure sub-optimal operations: i.e, steady state operations at the equilibrium. The next section aims to propose the PI- controller, $\mathbf{r}$, based on passivity techniques, in order to ensure that the converged equilibrium equals the desired *optimal* equilibrium point where control objective *1* and *2* are simultaneously satisfied.

# 3 Passivity Based Secondary Controller

The dynamics of the passivity based (PB) secondary controller are introduced in this section, aiming to ensure steady state operations at the equilibrium point where the conditions of the MG are restored. The definition of passive systems and passivity based controllers (PBC) are presented in the associated specialization project and in *Appendix* E for the reader of this thesis. The dynamics of secondary controller are therefore designed so that the closed loop MG converges to its steady state equilibrium, previously assumed to exist in *Assumption* 1, while simultaneously satisfying the two control objectives. The electrical network is already proven to converge to its steady state equilibrium. The distributed control network is therefore assessed at the equilibrium with the implemented PB PI-control dynamics. Hence, the dynamics of the secondary controller ensures that the cyber layer achieves steady state operations.

The cyber controller is previously defined equal to the output of the electrical network: i.e., the generated currents, interconnected through added weights $\mathbf{w}^{-1}$. This is presented in Figure 2.2 and in the closed loop control system given in 2.11. The cyber controller $\mathbf{u}_c$ is subsequently modelled in order to satisfy the steady state equilibrium conditions of the control network, defined as the point where the time derivative cyber states are zero: i.e., $\dot{\bar{\mathbf{x}}}_c = \mathcal{L}\bar{\mathbf{u}}_c = 0$. The time-dependent cyber states are defined as $\dot{\mathbf{x}}_c = \mathbf{g}_c \mathbf{u}_c$ where $\mathbf{g}_c = -\mathbf{K}_I \mathcal{L}$. $\mathbf{K}_I$ is the integral gain of the PI-controller and is previously defined as a positive definite diagonal matrix. Hence, the cyber controller needs to satisfy the equation below in order to ensure the steady state equilibrium.

$$\dot{\bar{\mathbf{x}}}_c = 0 \rightarrow \mathbf{g}_c \mathbf{u}_c = 0 \rightarrow -\mathbf{K}_I \mathcal{L} \mathbf{u}_c = 0 \rightarrow \mathcal{L}\bar{\mathbf{u}}_c = 0 \rightarrow \bar{\mathbf{u}}_c = \alpha \mathbf{1} \tag{3.1}$$

By using the properties of the Laplacian matrix, $\mathcal{L}\mathbf{1} = 0$ and $\mathbf{1}^\top \mathcal{L} = 0$, the cyber layer will converge in steady-state to a common consensus value, $\alpha = u_{opt}$. The cyber controller at the equilibrium is then given as: $\mathcal{L}\bar{\mathbf{u}}_c = 0 \rightarrow \bar{\mathbf{u}}_c = \bar{\mathbf{u}}_{opt} = u_{opt}\mathbf{1} \rightarrow \mathcal{L}u_{opt}\mathbf{1} = 0$. Knowing that the different inputs of the controller $\mathbf{u}_c$ will converge to a consensus value in steady-state, it is convenient to force them to be equal to the incremental cost vector. Towards this end, the cyber controller of the closed loop control system in 2.11 is then defined at the equilibrium as:

$$\bar{\mathbf{u}}_c = (\mathbf{w}^{-1})^\top \bar{\mathbf{y}}_{tot} + \mathbf{b}_c \rightarrow u_{opt}\mathbf{1} = (\mathbf{w}^{-1})^\top \bar{\mathbf{y}}_{tot} + \mathbf{b}_c \tag{3.2}$$

From the previously defined stationary conditions, the incremental costs of generation are expressed as: $\boldsymbol{\lambda} =$

$2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} + \boldsymbol{\beta}$. In order to rewrite the stationary conditions the three matrices $\boldsymbol{\lambda}$, $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ are defined below.

$$\boldsymbol{\lambda} = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix}, \ \boldsymbol{\beta} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix}, \ \boldsymbol{\alpha} = \begin{bmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_4 \end{bmatrix} \tag{3.3}$$

As previously discussed in Section 2.5, the output value of the electrical network equals the generated currents of each DG giving that $\mathbf{y}_{tot} = \mathbf{I}^{\mathcal{G}}$. The incremental costs at the equilibrium point of the MG, is now redefined in 3.4 by using the above matrices and the control objective *1* where $\lambda_i = \lambda_j = \lambda_{opt} \rightarrow \boldsymbol{\lambda} = \lambda_{opt}\mathbf{1}$.

$$\bar{\boldsymbol{\lambda}} = 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot} + \boldsymbol{\beta} = \lambda_{opt}\mathbf{1} \tag{3.4}$$

It is concluded that the distributed control system achieves steady state equilibrium when the MG is of closed loop, where all the generating units achieve consensus upon their incremental costs of generation. The next section proves that the above derivations, combined with the *Definition* 1, ensures that the final control system stabilizes to a steady state equilibrium point satisfying the two control objectives simultaneously.

**Definition: 1.** *The constants:* $\mathbf{b}$, $\mathbf{b}_c$, *control dissipation:* $\mathbf{r}$, *and weightings in the power preserving interconnections:* $\mathbf{w}^{-1}$, *are proposed equal to*

$$\mathbf{b} = -K_p\mathbf{w}^{-1}\mathcal{L}\boldsymbol{\beta}, \quad \mathbf{b}_c = \boldsymbol{\beta}, \quad \mathbf{r} = -\mathbf{R}^D + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}, \quad \mathbf{w}^{-1} = 2\boldsymbol{\alpha}.$$

## 3.1 Stability of Cyber-Physical MG with Passivity Based Secondary Controller

*Appendix* D includes the Lyapunov stability proof of the closed loop MG: i.e., when the secondary controller is operating. However, the inherent dynamics of the PI-controller $\mathbf{r}$ are not implemented and the proof only considered the controller to be implemented in the total dissipation matrix $\mathbf{T}_T = \text{blockdiag}((\mathbf{R}^{\mathcal{G}} + \mathbf{R}^D + \mathbf{r}), \mathbf{R}^{\mathcal{E}}, \mathbf{G}^{\mathcal{N}}_{cte}) \in \mathbb{R}^{3\times3}$. When $\mathbf{r} = -\mathbf{R}^D + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}$ the droop control is cancelled out and the new dissipation matrix is defined as $\mathbf{T}_T = \text{blockdiag}((\mathbf{R}^{\mathcal{G}} + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}), \mathbf{R}^{\mathcal{E}}, \mathbf{G}^{\mathcal{N}}_{cte}) \in \mathbb{R}^{3\times3}$. $K_P$ is a scalar gain defined as a positive value and the Laplacian is always defined as a positive definite matrix, proven with square-matrix properties and the *Gershgorin Circle Theorem* given in *Appendix* E. $\mathbf{T}_T$ is therefore defined as a positive definite matrix if $\boldsymbol{\alpha}$ is implemented as positive definite. The further stability analysis is therefore based on the *Assumption*:

**Assumption: 2.** *The matrix containing the primary control parameters is defined as positive definite,* $\boldsymbol{\alpha} > 0$.

The Lyapunov candidate is expressed equally as in *Appendix* D, however, the inherent dynamics of the PI-controller $\mathbf{r}$ is now included in the dissipation matrix:

$$\begin{aligned} V_T(\tilde{x}_T) &= H_{tot}(\tilde{x}_{tot}) + H_c(\tilde{x}_c) \\ &= \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top\mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top\mathbf{K}_I^{-1}\tilde{\mathbf{x}}_c \end{aligned} \tag{3.5}$$

$$\dot{V}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top V_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}^\top V_{tot}(\tilde{x}_{tot}) \tag{3.6}$$

The Lyapunov candidate is therefore concluded a certified Lyapunov function: i.e., a stability certificate when *Assumption* 2 holds. Due to the fact that $\mathbf{T}_T$ now is defined as positive definite, the stability conclusion drawn in *Appendix* D is equally valid with the implemented dynamics of $\mathbf{r}$. The CP MG is then proven to converge to a steady state equilibrium certified to be the *optimal* operating point. Equilibrium analyses are then conducted, evaluating if the two control objectives are satisfied at the *optimal* equilibrium with the proposed control dynamics.

### 3.1.1 Proof that the Cyber Controller Satisfies Control Objective *1* at the Equilibrium Point

With the above *Definition* 1 the closed loop control system, defined at the equilibrium, is expressed as:

$$\bar{\mathbf{u}}_{tot} = -\mathbf{r}\bar{\mathbf{y}}_{tot} - 2\boldsymbol{\alpha}\bar{\mathbf{y}}_c + \mathbf{b} \tag{3.7}$$

$$\bar{\mathbf{u}}_c = 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot} + \boldsymbol{\beta} \tag{3.8}$$

The control values and incremental costs at the equilibrium are defined as equal to the consensus value substitution the proportional current-sharing objective as shown in 2.4.

$$\bar{\mathbf{u}}_c = u_{opt}\mathbf{1} = 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot} + \boldsymbol{\beta} = \lambda_{opt}\mathbf{1} = \bar{\boldsymbol{\lambda}} \tag{3.9}$$

Hence, the proposed controller satisfies the KKT conditions at the equilibrium bringing the system to steady state stability while satisfying the control objective *1*, due to:

$$u_{opt} = \lambda_{opt} \quad \text{and} \quad \bar{\lambda}_i = \lambda_{opt} \tag{3.10}$$

### 3.1.2 Proof that the Secondary Controller Satisfies Control Objective *2*

The decentralized droop control dynamics are defined in 1.7 as: $\mathbf{V} = \mathbf{1}V_{nom} - \mathbf{R}^D\mathbf{I}^{\mathcal{G}} + \mathbf{u}_{tot}$. The objective of the droop control is to regulate the voltage output of the DGs, representing the primary voltage regulation in the electrical network. The primary controller at the equilibrium point of the MG is therefore expressed as:

$$\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \bar{\mathbf{u}}_{tot} \tag{3.11}$$

In order to ensure that the closed loop control system defined in 2.11 satisfies the control objective *2*, the the secondary control value, $u_{tot}$ is expressed at the equilibrium with the dynamics proposed in *Definition* 1: $\bar{\mathbf{u}}_{tot} = -\mathbf{r}\bar{\mathbf{y}}_{tot} - (\mathbf{w}^{-1})\bar{\mathbf{y}}_c + \mathbf{b}$. This secondary controller is then implemented in the voltage control dynamics of the physical layer at the equilibrium, presented in 3.12. This is carried out in order to assess if the obtained voltage controller brings the electrical network to an equilibrium where weighted average voltage regulation is ensured.

$$\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{y}}_{tot} - \mathbf{r}\bar{\mathbf{y}}_{tot} - (\mathbf{w}^{-1})\bar{\mathbf{y}}_c + \mathbf{b} \tag{3.12}$$

Multiplying by the sum of the voltage weightings $\mathbf{1}^\top\mathbf{w}$ on each side, we get:

$$\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\left[(\mathbf{R}^D + \mathbf{r})\bar{\mathbf{y}}_{tot} + \mathbf{w}^{-1}\bar{\mathbf{y}}_c - \mathbf{b}\right] \tag{3.13}$$

The dynamics defined in *Definition* 1 are now replaced in the above equality. $\mathbf{r} = -\mathbf{R}^D + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}$ where $K_p > 0$ is the proportional gain of the PI-controller and $\mathbf{b} = -K_p\mathbf{w}^{-1}\mathcal{L}\boldsymbol{\beta}$ is the added constants. With the defined weightings and proposed controller, average voltage regulation is reached in steady state if $\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom}$.

$$\mathbf{1}^\top\mathbf{w}\bar{V} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\left[(\mathbf{R}^D + (-\mathbf{R}^D + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}))\bar{\mathbf{y}}_{tot} + K_p\mathbf{w}^{-1}\mathcal{L}\boldsymbol{\beta}\right] - \mathbf{1}^\top\bar{\mathbf{y}}_c \tag{3.14}$$

$$= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\left[K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}\bar{\mathbf{y}}_{tot} + K_p\mathbf{w}^{-1}\mathcal{L}\boldsymbol{\beta}\right] - \mathbf{1}^\top\bar{\mathbf{y}}_c \tag{3.15}$$

The two terms inside the brackets equals to zero due to the Laplacian property $1^\top\mathcal{L} = 0$ and $K_p$ defined as a scalar constant: The term $-\mathbf{1}^\top\mathbf{w}K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}\bar{\mathbf{y}}_{tot} = -K_p\mathbf{1}^\top\mathcal{L}\mathbf{w}^{-1}\bar{\mathbf{y}}_{tot} = 0$, and similarly $-K_p\mathbf{1}^\top\mathcal{L}\boldsymbol{\beta} = 0$. The last term can be expressed as: $\mathbf{1}^\top\bar{\mathbf{y}}_c = -\mathbf{1}^\top\mathcal{L}\mathbf{K}_I\boldsymbol{\nabla}H_c(\bar{x}_c) = -\mathbf{1}^\top\mathcal{L}\mathbf{K}_I\mathbf{K}_I^{-1}\bar{\mathbf{x}}_c = -\mathbf{1}^\top\mathcal{L}\bar{\mathbf{x}}_c$ by using the definition of the control network in 2.10. The last term is therefore also equal to zero due to the the same Laplacian property.

With the passivity based controller presented in *Definition* 1, the weighted voltage regulation is expressed at the equilibrium of the physical network as: $\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom}$. It is then valid to conclude that the control system ensures that objective *2* is satisfied at the converged equilibrium point of the MG.

To summarize: The new closed loop control system represented in 2.11 combines both primary and secondary control. It is first proven that the cyber controller brings the distributed control network to the equilibrium point, where all the generating units cooperatively define the consensus value bringing the time derivative of the cyber states to zero. It is therefore concluded that the cyber controller ensures that the control objective *1*: i.e, proportional current-sharing is satisfied at the converged equilibrium point. Finally, it is shown that the PB PI-controller in the closed loop control system ensures voltage regulation by cancelling out the decentralized droop control in DGs and establishing a new secondary controller ensuring the control objective *2*: i.e., weighted average voltage regulation, at the converged equilibrium.

## 3.2 Proposed Distributed Controller in Scalar Form

The control system presented in 2.11 are now combined with the control dynamics in *Definition* 1 in order to express the control system in a more compact form. This will simplify the notation of the two controllers

and allows for later implementation of the control system in actual dynamical systems and in simulations. An additional advantage of this representation is the underscoring of the Laplacian matrix. As previously defined, the Laplacian matrix contains the consensus properties and describes the communication topology. This will later be beneficial when cyber attacks are assessed as a perturbation within the cyber layer.

As previously defined the secondary controller delivered to the electrical network is given as:$\mathbf{u}_{tot} = -\mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c + b$ and the cyber controller is given as:$\mathbf{u}_c = \mathbf{w}^{-1^\top}\mathbf{y}_c$. With the proposed controller where $\mathbf{w}^{-1} = 2\boldsymbol{\alpha}$, $\mathbf{b}_c = \boldsymbol{\beta}$, $\mathbf{r} = -\mathbf{R}^D + K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha}$ and $\mathbf{b} = -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta}$ the control values may be expressed as below. Recalling that the output of the electrical network is defined equal to the generated currents in each DG giving that $\mathbf{y}_{tot} = \mathbf{I}^{\mathcal{G}}$ and that the output of the cyber layer, $\mathbf{y}_c$ is defined equal to $\mathbf{g}_c^\top \boldsymbol{\nabla} H(x_c) = -\mathbf{K}_I \mathcal{L} \mathbf{K}_I^{-1} \mathbf{x}_c = -\mathcal{L}\mathbf{x}_C$.

$$\mathbf{u}_c = 2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} + \boldsymbol{\beta} \tag{3.16}$$

$$\begin{aligned}\mathbf{u}_{tot} &= -(-\mathbf{R}^D + K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha})\mathbf{y}_{tot} - 2\boldsymbol{\alpha}\mathbf{g}_c^\top \mathbf{y}_c^+ K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ &= \mathbf{R}^D\mathbf{I}^{\mathcal{G}} - 2\boldsymbol{\alpha}(K_p\mathcal{L}2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} - \mathcal{L}\mathbf{x}_c + K_p\mathcal{L}\boldsymbol{\beta})\end{aligned} \tag{3.17}$$

To further simplify the notation of the controllers, $\mathbf{z}^\lambda$ and $\mathbf{z}^c$ are defined below.

$$\mathbf{z}^\lambda = \begin{bmatrix} z_1^\lambda \\ z_2^\lambda \\ z_3^\lambda \\ z_4^\lambda \end{bmatrix} = -\mathcal{L}\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix} = -\mathcal{L}\boldsymbol{\lambda} \tag{3.18}$$

$$\mathbf{z}^c = \begin{bmatrix} z_1^c \\ z_2^c \\ z_3^c \\ z_4^c \end{bmatrix} = -\mathcal{L}\begin{bmatrix} x_1^c \\ x_2^c \\ x_3^c \\ x_4^c \end{bmatrix} = -\mathcal{L}\mathbf{x}_c \tag{3.19}$$

The final control values are then represented below with the new parameters and by using the definition of the incremental costs, previously obtained from the stationary conditions as $\boldsymbol{\lambda} = 2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} + \boldsymbol{\beta}$.

$$\mathbf{u}_{tot} = \mathbf{R}^D\mathbf{I}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}(2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} + \boldsymbol{\beta}) + \mathcal{L}\mathbf{x}_c) \tag{3.20}$$

$$= \mathbf{R}^D\mathbf{I}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\lambda + \mathcal{L}\mathbf{x}_c) \tag{3.21}$$

$$= \mathbf{R}^D\mathbf{I}^{\mathcal{G}} + 2\boldsymbol{\alpha}(K_p\mathbf{z}^\lambda - \mathbf{z}^c) \tag{3.22}$$

This new secondary control definition is expressed in scalar notation below.

$$u_{tot,i} = R_i^D I_i^{\mathcal{G}} + 2\alpha_i(K_p z_i^\lambda - z_i^c) \tag{3.23}$$

The introduced parameters $\mathbf{z}^\lambda$ and $\mathbf{z}^c$ include the Laplacian matrix. Hence, the parameters dependent on the topology of communication Graph 3 defining which nodes constitute neighbouring units: i.e., the units that are communicating and sharing information. The parameter values of each individual unit $i$ are dependent on only the neighbours' incremental costs $\lambda_j$ or neighbours' controller states $x_j^c$ where the neighbouring units are defined in the Adjacency matrix of Graph 3 given in 2.6. The individual parameter values for unit $i$ are then defined:

$$z_i^\lambda = \sum_{j\in\mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) \tag{3.24}$$

$$z_i^c = \sum_{j\in\mathcal{N}_c} a_{ij}(x_j^c - x_i^c) \tag{3.25}$$

For the case specific microgrid the secondary control dynamics of each individual DG are given as:

$$DG1: \begin{cases} u_1 = R_1^D I_1^{\mathcal{G}} + 2\alpha_1(K_p z_1^\lambda - z_1^c) \\ \dot{x}_1^c = K_1^I z_1^\lambda \\ z_1^\lambda = \lambda_2 - \lambda_1 \\ z_1^c = x_2^c - x_1^c \\ \lambda_1 = 2\alpha_1 I_1^{\mathcal{G}} + \beta_1 \end{cases} \quad DG2: \begin{cases} u_2 = R_2^D I_2^{\mathcal{G}} + 2\alpha_2(K_p z_2^\lambda - z_2^c) \\ \dot{x}_2^c = K_2^I z_2^\lambda \\ z_2^\lambda = (\lambda_1 + \lambda_3 + \lambda_4) - 3\lambda_2 \\ z_2^c = (x_1^c + x_3^c + x_4^c) - 3x_2^c \\ \lambda_2 = 2\alpha_2 I_2^{\mathcal{G}} + \beta_2 \end{cases} \tag{3.26}$$

$$DG3: \begin{cases} u_3 = R_3^D I_3^{\mathcal{G}} + 2\alpha_3(K_p z_3^\lambda - z_3^c) \\ \dot{x}_3^c = K_3^I z_3^\lambda \\ z_3^\lambda = (\lambda_2 + \lambda_4) - 2\lambda_3 \\ z_3^c = (x_2^c + x_4^c) - 2x_3^c \\ \lambda_3 = 2\alpha_3 I_3^{\mathcal{G}} + \beta_3 \end{cases} \quad DG4: \begin{cases} u_4 = R_4^D I_4^{\mathcal{G}} + 2\alpha_4(K_p z_4^\lambda - z_4^c) \\ \dot{x}_4^c = K_4^I z_4^\lambda \\ z_4^\lambda = (\lambda_2 + \lambda_3) - 2\lambda_4 \\ z_4^c = (x_2^c + x_3^c) - 2x_4^c \\ \lambda_4 = 2\alpha_4 I_4^{\mathcal{G}} + \beta_4 \end{cases}$$

# 4 Simulations of Interconnected Microgrid

The distributed control network with the proposed secondary passivity based PI- controller is now implemented in Simulink. The simulations are conducted with the intention of validating that the controller is able to ensure optimal operations of the MG, as mathematically proven above. In the specialisation project, the electrical network was simulated and tested with respect to stability. The simulations of the electrical network were based on the presented model with four generating units, four power consuming loads and five transmission lines. The simulations in this thesis – with the new distributed control network – the generators are additionally connected in the distributed control network through the specified interconnection pattern. The control network establishes communication between the four generating units, and the inherent dynamics implemented in Simulink are defined in 3.26describing the dynamics of the cyber layer. The closed loop control system is subsequently simulated and the control performance is tested for some defined events that may perturb the operations of the electrical system. The simulated events are presented in Table 4.1. They are implemented as step changes in specified time intervals, in order to simulate the severe changes within the electrical system. The performance of the physical network controlled by the primary droop controller is simulated with the same occurring events, in the associated specialization project. All the necessary parameter variables are presented in *Appendix* A.

Table 4.1: Events occurring in inherent dynamics of electrical network

| Time Interval [seconds] | Event | Location |
|---|---|---|
| [3, $\infty$] | Activation of Secondary Controller | Coherent to all DGs |
| [6, 9] | Increased Current Consumption | Load 1 |
| [12, 15] | Decreased Current Consumption | Load 4 |
| [18, 21] | Impedance Increase | Load 1 |
| [24, 27] | Impedance Increase | Load 2 |

As can be observed from the table above, the distributed secondary controller is activated at time step 3 seconds. Recall that the desired system response is a stable system, ensuring steady state operations at the equilibrium of the system where both the average voltage regulation and the equal incremental cost objectives are ensured when the secondary controller is activated. The control parameters implemented in the simulation model of the distributed controller is presented in the Table 4.2. Even though $\mathbf{K}_I$ is defined as $\mathbf{K}_I = \text{diag}\{K_i^I\} \in \mathbb{R}^{4\times4}$ the Table 4.2 presents that the simulations integrate the cyber states with the same integrator gain accelerating the consensus property. $K_P$ is implemented as a scalar gain equal for all DGs. $\alpha$ is the control parameter in regards to the incremental costs of the DGs where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are implemented with individual ratings influenced by the values presented in Babak's publication *Distributed Control and Optimization of DC Microgrids: A Port-Hamiltonian Approach* [1].

Table 4.2: Control parameters

| Control Parameters | Associated to DG number i $\in \mathcal{G}$ | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| $K_p$ | 2 | | | |
| $K_I$ | 100 | | | |
| $\alpha$ | 0.8 | 1.9 | 1 | 1.4 |
| $\beta$ | 1 | 2.5 | 1.2 | 1.8 |

The figures below present the system response of the simulated events with the implemented distributed control system. Firstly the average voltage control objective is assessed. In order to plot the average of all the DG's voltages, the weighted sum of the voltages needs to be calculated and plotted for each time step. The second control objective is previously defined in scalar form as $\lim_{t\to\infty} \sum_{i\in\mathcal{G}} \mathbf{w}_i \bar{V}_i = V_{nom} \sum_{i\in\mathcal{G}} \mathbf{w}_i$ which is expressed in vector notation as $\mathbf{1}^\top \mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top \mathbf{1} V_{nom}$. Remembering that $\mathbf{w} = \frac{1}{2\boldsymbol{\alpha}}$ and the final average voltage regulation

is, for the case specific MG, represented as:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2\alpha_1} & 0 & 0 & 0 \\ 0 & \frac{1}{2\alpha_2} & 0 & 0 \\ 0 & 0 & \frac{1}{2\alpha_3} & 0 \\ 0 & 0 & 0 & \frac{1}{2\alpha_4} \end{bmatrix} \begin{bmatrix} \bar{V}_1 \\ \bar{V}_2 \\ \bar{V}_3 \\ \bar{V}_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2\alpha_1} & 0 & 0 & 0 \\ 0 & \frac{1}{2\alpha_2} & 0 & 0 \\ 0 & 0 & \frac{1}{2\alpha_3} & 0 \\ 0 & 0 & 0 & \frac{1}{2\alpha_4} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} V_{nom} \tag{4.1}$$

So in order to test if the MG is achieving a weighted voltage sum equal to the nominal voltage of 48 $V$, the equation above is solved with respect to the nominal voltage. The three first matrices appearing after the equality will be equal to the sum of the weightings of each DG, given as a scalar. Hence, $V_{nom}$ may be represented as the weighted sum of each measured voltage of the four DGs divided by the scalar sum of the weightings. The final equation used to plot the performance of the voltage controller is then defined as:

$$V_{nom} = 2\frac{\frac{\bar{V}_1^{\mathcal{G}}}{2\alpha_1} + \frac{\bar{V}_2^{\mathcal{G}}}{2\alpha_2} + \frac{\bar{V}_3^{\mathcal{G}}}{2\alpha_3} + \frac{\bar{V}_4^{\mathcal{G}}}{2\alpha_4}}{\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} + \frac{1}{\alpha_4}} \tag{4.2}$$

The associated voltage control plot will ideally show a function of the weighted sum equal to 48 $V$ for all time steps when the secondary controller is activated. It is then possible to conclude that the voltage control objective is satisfied. However, if the sum is not equal to 48 $V$, the system is not reaching the desired voltage control due to potential faults in the system e.g. cyber attacks. This is later studied for several types of attacks potentially affecting the effectiveness of the voltage regulations.

Figure 4.1: Unforced MG with secondary control

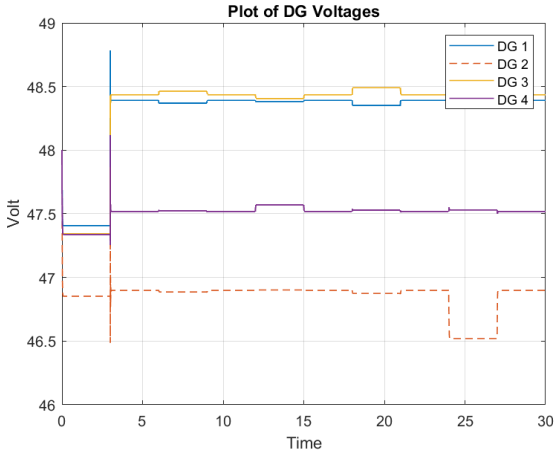


Figure 4.2: DG voltages of unforced system

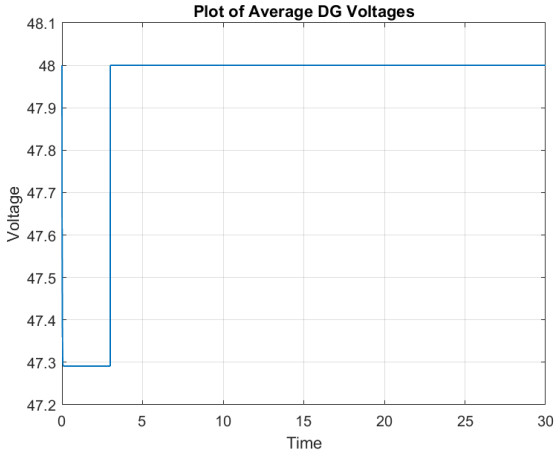


Figure 4.3: Average voltage of the unforced system

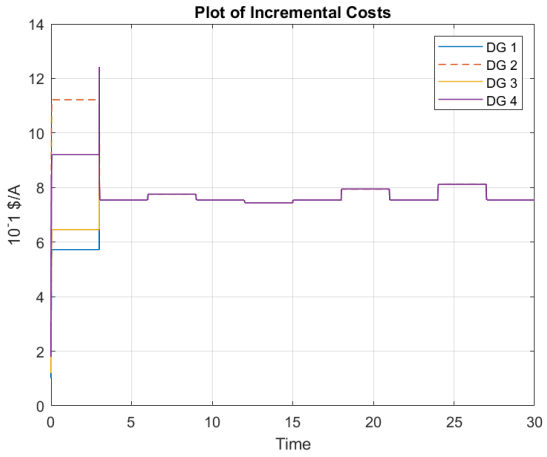


Figure 4.4: Incremental costs of unforced system

Figure 4.2 and 4.3 shows the voltage performance of the case specific MG. Figure 4.2 plots the voltages of each DG, showing that all the generating units have steady state operations before, during and after the simulated

step changes. By studying the changes in the voltage for the different events, it is shown that if one of the DGs has a droop in the voltage, the other units will try to compensate for this droop by increasing their voltages, ensuring that the average voltage always is equal to the nominal voltage $48V$. In Figure 4.3 this is validated as the sum of the voltages is equal to 48V for all the time steps when the secondary controllers are activated. By studying the time interval $[0, 3]$ seconds, it is shown that without the secondary controller the system is able to operate at steady state but is not able to ensure average voltage regulation as the MG is only controlled by the droop, limiting the violations but not restoring system conditions. The last figure shows the plotted incremental costs of the DGs for all the time steps. Before the secondary controller is activated: i.e., in the time interval $[0, 3]$ seconds, it is also shown that neither the control objective *1* is satisfied as the units do not achieve one value for the incremental costs. However, when the secondary controller is activated as 3 seconds, the units exploit the communication in the cyber layer and manage to cooperatively define one consensus value. The Figure 4.4 validates that all the DGs established the same incremental cost for all the simulated system changes.

# 5 Concluding Remarks on the Final Cyber-Physical MG Model

Implemented in *Part A* of this thesis, both mathematically conducted proofs and simulations are used to validate and present the motivation behind the energy modelling of complex cyber-physical microgrids. The proposed control dynamics are based on passivity, exploiting energy analysis when the model is developed. This simplifies the stability assessment as the controller is based on the main assumption that the power is preserved within the MG. The secondary control configurations are then proven to operate the MG at the desired steady state equilibrium where both the average voltage regulation and equal incremental costs criteria are satisfied. The distributed control network exploits the cyber-physical properties: i.e., exploiting communication within the cyber layer, in order to cooperatively establish the optimal operations of the MG. The performance of the MG is then mathematically proven optimal and validated by the simulations. The secondary controller is proven adaptive as the desired operations are maintained regardless of inherent system changes.

## Part B:

# Complex Cyber-Physical Microgrids: Under Cyber Attacks

The energy modelling and suitable design of the closed loop DC MG is so far completed and we have established a microgrid converging to optimal steady state. The primary and secondary controller is merged into one closed loop control system exploiting both distributed and decentralized control configurations. The distributed control scheme provides operational advantages, previously defined as scalability and reliability. However, the integration of communication and automation technologies increases the vulnerability of cyber threats attacking the cyber-physical MG. These vulnerabilities allow potential attackers to create unfavorable scenarios, which may lead to uneconomic operation, instability or system shutdown [13]. Hence, due to the limited global information and vulnerabilities in the communication links, distributed control systems are prone to cyberattacks causing additional challenges in regards to control system modelling [14]. In order to provide privacy and security in the CP MG the distributed control algorithm needs to be modelled aiming to ensure one additional control objective: *Resilience against cyber threats*.

The first section implemented in *Part B* is a literature review on potential cyber attacks in electrical power systems. The study focuses on different types of cyber attacks, how they malign the electrical power systems and studies necessary requirements in order to reduce the effect of the cyber threats. Subsequently, the case specific MG is assessed as a perturbed system prone to all types of cyber attacks. Three chosen attacks are then implemented as perturbations of the MG and the control resilience is evaluated, aiming to establish a robust controller reducing the affect of the vicious attacks regardless of where the attack is intruding the MG and regardless of type of threats. *Part B* will therefore present the theoretical study on perturbed systems exposed to cyber threats, followed by in depth analyses of the systems operational destruction entailed by the attacks and how to accordingly reduce the destruction caused by the attack. In addition, *Part B* will show the reader how to properly implement cyber threats to electrical power systems, as it is a sophisticated operation requiring prerequisite knowledge of the dynamical details of the cyber-physical power systems.

# 1 Cyber Security in Power Systems

When electrical power systems exploits communication within the controllers, the networks becomes prone to cyber attacks threatening the control performance and thereby the optimal operations of the MG. These cyber threats will perturb through attack vectors aiming to disturb the steady state operations or prevent the power system of converging to optimal operations [15]. Resilient control strategies are therefore studied and proposed as solutions aiming to reduce the drawbacks caused by the attacks. In the existing literature, various detection algorithms have been proposed, specified for the individual type of cyber attacks. These detection algorithms are used in the design of several controllers, resulting in resilient controllers robust against specified cyber threats by firstly identifying and then removing the attacks as fast as possible. In the literature the most researched types of potential cyber threats are: *false data injection attack* (FDIA), *denial- of - service attack* (DoS), *stealth attack* and *man-in-the-middle attacks* (MITM) [14].

In order to address the resilience strategies against the unknown cyber attacks, several attack-detection and mitigation techniques have been developed and robust distributed control systems have been researched. The main focus of the proposed techniques is to detect, identify and then remove the misbehaving units within the MG [16]. The proposed strategy in this thesis will instead focus on novel resilience: i.e., robust against all types of cyber threats without needing to detect and mitigate perturbed units.

## 1.1 False Data Injection Attacks

The false data injection attacks (FDIA) are one type of the most prominent attacks in the existing literature. The attack propagates the system signals by adding false information on top of existing signals in either the controllers (primary and/or secondary), the actuators of the controllers, in the measuring devices or in communication links in the cyber layer [13]. The most researched types are FDIA in the current sensors, *stealt* attacks in voltage sensors or *Denial - of - Service* attacks (DoS) in large scale power systems. As FDIAs only adds data on top of existing signals, the MG may still reach agreement, however the final consensus values may be incorrect and the desired control objectives of the power system may not be satisfied or optimized [13].

There exist several detection algorithms for detecting FDIAs, and in existing literature the FDIA are often designed to attack the current sensors or in the communication links of the control architecture. Attacks on voltage sensor measurements are often designed as Stealth attacks [17], which has a more discreet behaviour by deceitfully penetrating into the control system and cause instability later in unforeseen ways [18].

In [15] a detection algorithm is proposed showcased in this section as one way to model a FDI detection algorithm. The algorithm aims to detect and mitigate the threats that propagate the already established detection and mitigation platforms implemented in the DGs. By attacking these platforms where the misbehaving DGs are identified and removed, the attacks are able to inject false information in the MG [14]. The detection algorithm is described as a framework, able to identify a change in the sets of presumed candidate invariants. Invariants are defined as a microgrid property that do not change over time [15]. The actual invariants of the MG are identified by a reachability analysis that generates a set of the reachable states of the grid. Then, by comparing the candidate invariants with the actual variants the presence of FDIAs are indicated by any mismatches in the comparison [15].

**Stealth Attacks**
Stealth attacks are considered the intelligent false data injection attack, where the consensus algorithm objectives of the secondary controller are satisfied while the distributed control system is under attack [17]. The stealth attacks need to be coordinated attacks where the attacker attains sufficient knowledge of the system including the control and network architecture in order to create the attack vector [18]. Hence, the stealth attacks are able to deceive the control system and propagate the system signals without being noticed by the system operator [17] and bypasses the bad-data detection test [18]. In [17] a stealth attack detection technique is proposed by calculating an attack index in the secondary controller, able to detect the potential stealth attacks in the current measurements. The proposed detection method is able to effectively identify the stealth attacks with existing low bandwidth communication.

Many of the proposed FDIA detection algorithms from existing literature like element approach-based detection technique [18], observer-based detection and mitigation approach [19] or the mentioned identification of candidate invariants require to communicate some additional information between the neighbouring units in order to detect the attacks. Hence, several proposed detection techniques requires consequently higher bandwidth within the communication network increasing the complexity of the network [17].

**Denial - of - Service Attacks**
The denial of service attacks interferes with the communication links by sending large unauthentic packages and thereby congesting the communication channels [20]. The DoS blocks the wanted transmitted packages and interrupts the regular communication for a period of time. The DoS attacks are often designed to infiltrate large scale power systems where the information exchanged between the sub-systems are transmitted over networks that generates heavy communication burden prone to cyber attacks. Hence, event triggered control techniques have been researched as a solution to avoid unnecessary utilization of communication resources and a solution to ensure resilience against DoS attacks [20]. In [20] an event-based secondary controller is designed where each DG communicates its information through the network channels only when the event triggering conditions are violated. In addition a switching framework is considered between the communication and attack intervals, ensuring sufficient conditions of the switching frequency and duration of the DoS cyber attacks. Hence, the event-based controller ensures detection of the attacks and the switching framework ensures that the DoS attacks will not have the operational time to prevent the desired objectives of the overall MG.

## 1.2 Hijacking Attacks

Hijacking attacks, also named *random attacks*, are another type of cyber attacks that infiltrates the communication network by changing the communicated data between the units. Hence, the cyber attacks are able to bring the MG to operate at other operational conditions than desired. In comparison of the mentioned faulty attacks adding false signals on top of the existing ones, the hijacking attacks completely replace the existing signals. As a result, the compromised agents diverge from steady state operations due to imbalance in the iterative consensus algorithm [13]. From existing literature it is shown that the attacks are able to prevent the MG to achieve optimal performance. The consensus algorithm is not able to update its reference state, with respect to its neighbouring unit, as the communicated data is replaced by a constant input, resulting in power imbalance. In order to design a resilient control system, detecting and mitigating the misbehaving unit, it is necessary to select the compromised unit. However, due to the consensus algorithm, all the units are misbehaving simultaneously while only one unit actually is compromised which causes difficulties in detecting where the attack is intruding the system. Hence, detection algorithms of hijacking attacks becomes more challenging than detecting the faulty attacks. In [13] a novel distributed screening (DS) methodology is proposed together with a fault detection (FD) metric. This combination provides a detection strategy that is able to differentiate between sensor attacks and hijacking attacks, reducing the complexity of decision making in the mitigation operations.

**MITM- attacks**
As the cyber layer is modelled with dynamical cyber-physical entities to the electrical MG, it is critical to detect the hijacked cyber links and mitigate the attack in order to prevent unreliable operations of the grid. One of the most prominent attacks in the cyber layer is the MITM attacks, involving infiltrating the communication links with tampered data packages with the intend of steering the microgrid toward inconsistent performance [21]. The infiltration is performed by a third party, and the attack may perturb the network by either adding false data or by hijacking the communication links, both preventing secure communication between the units [21].

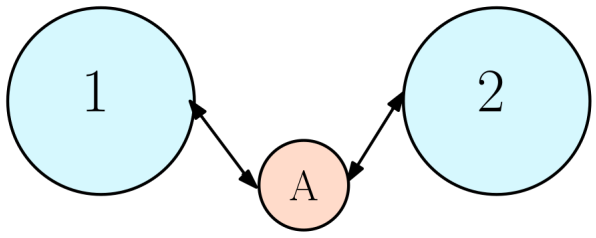


Figure 1.1: Man-in-the-middle attack

A simple visualization of a MITM attack is shown in Figure 1.1. The third party attacker, A, infiltrates the communicated data between node 1 and 2, achieving to operate as the proxy server between the units. Hence, the attacker has the opportunity to either intercept the incoming information (hijacking attack) or malign both incoming and outgoing information between the two nodes (false data injection attack)[21]. When the attack is modelled as a hijacking attack the compromised agent(s) diverge from the optimal steady state operation as there will be imbalance in the iterative rule of consensus algorithm [13].

In [21] a multilayer event-driven resilient controller is proposed in order to to detect and mitigate MITM attacks immediately [21]. The controller identifies the presence of an attack in a cyber link by using a diverging factor based detection law. Then a detection metric is created containing the malicious signals in voltage and current counterparts. The event-driven controller is then activated when the direction metric rises beyond a very small threshold. As long as these events are activated in the compromised cyber link, an event-triggered signal is constructed using trusted control input error signals in the compromised unit. This control inputs are credible and trusted signals between the neighbouring units, authenticated prior to the event activation with a *true/false* signature.

This formulates the first layer of resilience against MITM attacks. However, if all the control input error signals in the neighbouring units of the compromised one are attacked, then the first layer of resilience is not robust against the several attacks. Hence, a multilayer resilience control scheme is proposed, only transmitting trusted control input error signals from neighbouring units that are authenticated as not under attack. Hence, the constructed event-triggered signal becomes credible ensuring resilience against the correct MITM attacked cyber link.

## 1.3 Critical Aspects of Existing Robust Control Schemes

The main problems in existing propositions regarding robust control schemes, are that the proposed attack-detection and mitigation approaches have limited abilities to accurately detect the attacks, identify the location, identify the type of attack and remove the threats before the attacks have compromised the reliability and stability of the MG. Also, detection and mitigation algorithms often require more dense topology within the cyber network, given that additional information needs to be communicated between the units. Hence, most of the existing robust control solutions require complex modelling configurations with a more dense communication system, increasing the complexity and economical expenses of the power system modelling.

Limitations, due to long detection time, constrain the applicability of detection algorithms as the reliability and stability operations may already been compromised before the worst-case attacks are detected and removed. Another critical aspect is the complexity of selecting the accurate compromised cyber link before performing any mitigation action [21]. Hence, it is important to ensure accurate, fast detection and mitigation techniques in order to prevent disrupting the stability and performance of the MG [14]. Furthermore it would not be possible to design a detection algorithm that is able to unmask all potential cyber threats in the cyber physical control network [16]. Hence, another solution is to design an adaptive cooperative control algorithm for multi-agent systems, resilient against unknown cyber attacks [22].

Several of the proposed algorithms struggle to constrain and limit the cyberattacks when most of or all of the DGs within the network are subject to cyber attacks. Hence, the detection and mitigation of the threats, when surplus DGs are compromised, may limit the stability and performance of the MG prone to worst-case attackers [14]. In the mentioned multilayered controller, the MITM detection and mitigation algorithms require several layers in order to ensure a resilient controller when several units are compromised. The advantage of the design is that the detection algorithm manages to operate the MG while several units are compromised. However, this is only achieved by adding several layers in the control model and additional communication links for the authentication signals, creating a a very complex control configuration with dense topology.

In addition to identify the type of attack and where the attack perturbs, the detection algorithms also needs to differentiate between the cyber attacks and potential faults in the electrical systems. In the mentioned event-trigger based algorithms the detection metrics may diverge beyond the threshold by faults occurring in the electrical components. In [18] this is resolved by using an evaluation theory assisting the proposed detection scheme to avoid false tripping of relays.

In order to disregard these mentioned applicability limitations of the proposed detection and mitigation algorithms, this thesis focuses on establishing a novel robust control configuration. The proposed control strategy will not require any information about the nature and/or location of the cyber attacks and do not have any restrictions of the number of malicious nodes [22]. The controller system is adaptive and resilient achieving to operate as close to steady state as possible while being under attack. Hence, the proposed robust controller disregards the limitations when applying attack - detection and mitigation algorithms, and thereby reduces the complexity of the controller.

# 2 Perturbed Systems

The main objective of this thesis is to model a resilient controller that forces the microgrid to operate as close to the equilibrium of the unperturbed system as possible while subject to cyber attacks. In order to establish the resilient controller, the DC microgrid firstly needs to be modelled as a linear system with additional external inputs. The unforced MG: i.e., there exists no forced inputs, is presented in 2.1 as an autonomous unperturbed linear system. This implies that the system is time invariant with no external inputs disturbing the first order states [23].

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} \tag{2.1}$$

When the new MG is modelled as a system subject to cyber attacks, it needs to be modelled as a *perturbed* system. For the multi variable case (MIMO): i.e., when the system is exposed to several independent inputs, the perturbed model is given in 2.2 [24]. The states will then depend on additional perturbation terms: i.e., the time-dependent inputs $\mathbf{B}\mathbf{x}(t)$ in addition to the implemented physical dynamics in $\mathbf{A}\mathbf{x}$ – only depending on the inherent states. The system representation of the MG further studied in this thesis, is based on the perturbed model of a general linear system defined as:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{x}(t) \tag{2.2}$$

$\mathbf{A}$ includes the intrinsic physical dynamics of the cyber-physical microgrid. It is Hurwitz i.e having all eigenvalues in the left half-plane, ensuring that the unforced system converges to stable operations. Supposing that the perturbation term satisfies the linear growth bound

$$\| \mathbf{B}\mathbf{x}(t) \| \leq \boldsymbol{\gamma} \| \mathbf{x} \| \qquad \forall t \geq 0, \forall \mathbf{x} \in D \tag{2.3}$$

where $\boldsymbol{\gamma}$ is a non-negative vector containing constants. $D$ is a domain of $\mathbb{R}^n$ containing the orgin of the system where $\mathbf{x} = \mathbf{0}$. Given the initial conditions $\mathbf{A}\mathbf{x}_0 = \mathbf{0}$ and $\mathbf{B}\mathbf{x}_0(t) = \mathbf{0}$ the orgin becomes an equilibrium of the system. The perturbation term could result from modelling errors, uncertainties or disturbances within the physical system [23]. In this thesis the perturbation term represents the external cyber attacks threatening the control system and the perturbed system is therefore expressed below as a time-dependent input with respect to the control input $\mathbf{u}$.

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u}(t) \tag{2.4}$$

The cyber-physical network is modelled as a first order system with a set of linear equations, giving a MIMO representation and the states time response is given below [24].

$$\mathbf{x}(t) = e^{\mathbf{A}(t-t_0)}\mathbf{x}(t_0) + \int_{t_0}^{t} e^{\mathbf{A}(t-\tau)}\mathbf{B}\mathbf{u}(\tau)\, d\tau \tag{2.5}$$

The above equation demonstrates that the states are dependent on a steady state term, given by the initial conditions and a transient time-dependent input term. Even though the perturbation term is typically unknown, the upper bound $\| \mathbf{B}\mathbf{u}(t_0) \|$ is often known [23] and used, in this thesis, to bound the steady state states of the network while the system is under attack. The system's stability and bounded states will then depend on the strength of the bounded input. Higher upper bounds increases the solution space for the steady state stability of the system. However, more restrictive bounds ensures that the *input - to - state* stability (ISS) is less conservative such that the converged equilibrium is closer to the desired equilibrium. ISS is further explained in the Section 2.2 below.

## 2.1 Bounded Attacks

When focusing on the stability of a cyber-physical micorgrid subject to cyber attacks, the type of bounded inputs needs to be defined. This is significant in order to later study how this bounded input will bound the system steady state. When the resilient controller is analysed, modified and tested in this thesis, the cyber attacks under consideration needs to satisfy *Assumption* 3. The later defined control system are proven resilient to only uniformly bounded attacks.

**Assumption: 3.** *Assume that all potential cyber attacks perturbing the microgrids can be modelled as unknown, yet uniformly bounded attacks.*

Previously defined in 2.5, the time response of the autonomous linear system in 2.4 contains a steady state term and time-dependent transient term regarding the external input. For a uniformly bounded input, the initial conditions are given as:$\mathbf{x}(t_0) =\| \mathbf{a} \|$ where $\| \mathbf{a} \| >\| \mathbf{B} \| > 0$ [23]. Using *Definition 4.3* from Khalil's book Nonlinear Control [23], the solution of states are defined to be uniformly bounded if there exists $\| \mathbf{c} \| > 0$ independent of $t_0$, and for every $\| \mathbf{a} \| \in (0, \| \mathbf{c} \|)$ there is $\| \boldsymbol{\beta} \|$, dependent on $\| \mathbf{a} \|$ but independent of $t_0$ such that:

$$\| \mathbf{x}(t_0) \| \leq \| \mathbf{a} \| \rightarrow \| \mathbf{x}(t) \| \leq \| \boldsymbol{\beta} \|, \ \forall\, t \geq t_0 \tag{2.6}$$

The states of the system are then uniformly bounded in $t_0$: i.e., the solution has a bound $\| \mathbf{a} \|$ that is independent of $t_0$ and valid for all $t \geq t_0$. Hence, the steady state solution is defined to exist within that upper bound of the attack. It is then possible to obtain that bound and establish a control system ensuring that the solution is stable for the value of $\mathbf{x}$ higher than the obtained value of $\| \mathbf{a} \|$.

For time-invariant systems it is sufficient to define a uniformly bounded attack as only bounded attack. This is due to the fact that the solution only will depend on the time interval $t - t_0$ [23]. However, in order to generate the most general proof as possible, creating stability certificates that may serve as a useful staring point for further studies assessing nonlinear dynamics, the bounded inputs are specified as uniformly bounded.

## 2.2 Stability of a Perturbed System

As previously described the states of the perturbed system are depending on the bound of the external inputs. Hence, the stability of the system will also be bounded enforced by that bounded input defined as the *Bounded-input-bounded-state* property. Considering an unforced autonomous linear system, $\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$ where $\mathbf{A}$ is Hurwitz and the system is proven to have a globally asymptotically stable equilibrium point at the orgin $\mathbf{x} = \mathbf{0}$. When the system is prone to bounded cyber attacks the time response of the states, described in 2.5, are now bounded by the attack as presented below [23]:

$$\| \mathbf{x}(t) \| \leq \mathbf{k} e^{-\boldsymbol{\lambda}(t-t_0)} \| \mathbf{x}(t_0) \| + \int_{t_0}^{t} \mathbf{k} e^{-\boldsymbol{\lambda}(t-t_0)} \| \mathbf{B} \| \| \mathbf{u}(\tau) \| \, d\tau \tag{2.7}$$

$$\leq \mathbf{k} e^{-\boldsymbol{\lambda}(t-t_0)} \| \mathbf{x}(t_0) \| + \frac{\mathbf{k} \| \mathbf{B} \|}{\boldsymbol{\lambda}} \sup_{t_0 \leq \tau \leq t} \| \mathbf{u}(\tau) \| \tag{2.8}$$

The estimate shows that with the zero-input response decays to zero exponentially fast while the zero-state response is bounded for every bounded input. The bound on the zero-state response is proportional to the bound of the input. The *sup* term represents the *supremum*: i.e., the least upper bound of the attack. Using the *Lemma* 4.5 in Khalil's book [23], stating that if the unforced system ha a globally exponentially stable equilibrium point at the orgin, the perturbed system is defined as *input-to-state stable*(ISS). The properties of ISS, valid for the uniformly bounded attack, are defined as [23]:

- For any bounded input $\mathbf{u}(t)$, the state $\mathbf{x}(t)$ is bounded
- If $\mathbf{u}(t)$ converges to zero as $t \rightarrow \infty$, so does $\mathbf{x}(t)$
- The orgin of the unforced system is globally asymptotically stable

Lyapunov's stability method is used in this thesis as the primary stability assessment. When the steady state analysis is conducted for the perturbed cyber-physical microgrid, the goal is to establish a certificate valid for the condition stating that: *if the states are bigger than a specified constant value equal to the least upper bound of the attack–defined to be non-infinite–then perturbed system achieves ISS if bounded by the external input, if* $\dot{V} \leq 0$ .

## 2.3 Additional Control Objective

When the control system is modelled with a distributed controller exploiting communication, the cyber-physical MG needs to be modelled as a perturbed system subject to external inputs implemented as cyber threats. The control system will then require another additional control objective to compensate for the potential destruction caused by the attack. The two main objectives are previously describes as ensuring proportional current-sharing when cooperatively establishing equal incremental costs of the generation, and average voltage

regulation due to the added weightings in the interconnections between the cyber and physical layer. When the system now is assessed as prone to cyber attacks, the additional control objective *3*, specified below, also needs to be ensured at the equilibrium. The control system will then have three different control objectives that needs to be satisfied at the steady state equilibrium in order to ensure proper and optimal operations of the MG.

**Control Objective 3:** *Resilience against cyber threats* (2.9)
The microgrid operates as close as possible to the unforced system while being perturbed by potential cyber attacks, regardless of the attack location

The analyses in part *Part B*and *Part C* are subsequently conducted with the intention of analysing the perturbed CP MG subject to three different cyber attacks and then assess if the three control objectives are ensured at the equilibrium. The robust controller require resilient functionalities described as bringing the MG to operate as uncompromised and as close to the steady state operations of the unforced system as possible. The Lyapunov framework is used in the energy modelling and stability proofs of the secondary controller. The implementation of the attack vectors and proven stability certificates will then be defined valid for any linear CP DC microgrid admitting the same dynamics independent on the initial conditions of the system.

## 2.4 Proposed Resilient Controller

The final objective of this thesis is to present a modified adaptive resilient control version of [1], ensuring proportional current-sharing and average voltage regulation while being under attack. The external attacks are assumed to be uniformly bounded, generating a steady state stability bound on the CP MG states. The proposed resilient controller is based on proper design and tuning of the existing control parameters, influenced by Mahdieh S. Sadabadi's conference paper [16] and article [14]. Furthermore, the distributed controller of [1] is based on passivity and control by interconnection techniques, proven both stable and able to operate the MG at the desired steady state equilibrium for any number of units. As a first approach, it seems reasonable to keep the control structure of [1] and assess if tuning techniques may be sufficient to mitigate the attack, and therefore robustify the control. In Mahdieh S. Sadabadi's research she proposes to tune the control parameters to significant high values and thereby force the MG to operate as prior to the attack. The DC MG dynamics under consideration are highly dependent on the control parameter $\boldsymbol{\alpha}$. The $\alpha$'s are appearing both in the inherent dynamics of the controller and in the interconnections between the two networks. In *Definition* 1, $\mathbf{w}^{-1}$ is defined equal to $\boldsymbol{\alpha}$ and the resilient controller is proposed by tuning the primary controller as defined in *Hypothesis* 1.

**Hypothesis: 1.** *The resilience is ensured when tuning the primary control parameter $\boldsymbol{\alpha}$ to a significant high value, removing the effect of the perturbation term and establishing a resilient controller robust against all cyber attacks*

The resilience *Hypothesis* above are only valid when *Assumption* 2 holds, and the Lyapunov stability certificates are valid stability conclusions for all linear power systems. The proposed resilient controller: i.e., tuning of $\boldsymbol{\alpha}$, are assessed with respect to achieving the two control objectives at steady state equilibrium. In addition, it is evaluated if this proposed controller is able to ensure resilience regardless the nature of the attacks. The performance of the proposed tuning is tested on the case specific MG, perturbed by three different cyber attacks. If the tuned secondary controller satisfies the stability conditions and ensures the two control objective at the equilibrium while being under attack, then the resilient controller is performing optimally in regards to stability and optimal MG operations. On the other hands, if the objectives are not ensured, then the resilience strategy is not sufficiently robust and the mathematical structure of the secondary controller will need to be modified in order to completely remove the influence of the attacks.

# 3 Linear System Representation

In order to test the resilient secondary controller, the cyber attacked CP MG firstly needs to be modelled. For each cyber attack studied in the sections below, the attack vector formulation and implementation approach is explained. As previously mentioned, the modelling of the attack vectors require prerequisite knowledge of the dynamical details of the cyber-physical power systems. In order to manufacture the appropriate attack vectors that are able to intrude and malign the cyber controller as discrete as possible, the linear cyber-physical MG showcasing all intrinsic dynamics needs to be known and is therefore presented in this section.

The autonomous linear power system of study is presented below using only vector notation, based on the electrical dynamics defined in 1.1.2, and the closed loop control network defined in 2.11.

$$\begin{bmatrix} \dot{\mathbf{I}}^{\mathcal{G}} \\ \dot{\mathbf{I}}^{\mathcal{E}} \\ \dot{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^c \end{bmatrix} = \begin{bmatrix} \frac{1}{\mathbf{L}^{\mathcal{G}}}\left[2\boldsymbol{\alpha}(-K_p\mathcal{L}2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \frac{1}{\mathbf{L}^{\mathcal{G}}}\left[-\mathcal{B}^{\mathcal{G}\top}\right] & \frac{1}{\mathbf{L}^{\mathcal{G}}}\left[2\boldsymbol{\alpha}\mathcal{L}\right] \\ 0 & \frac{1}{\mathbf{L}^{\mathcal{E}}}\left[-\mathbf{R}^{\mathcal{E}}\right] & \frac{1}{\mathbf{L}^{\mathcal{E}}}\left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \frac{1}{\mathbf{C}^{\mathcal{N}}}\left[\mathcal{B}^{\mathcal{G}}\right] & \frac{1}{\mathbf{C}^{\mathcal{N}}}\left[\mathcal{B}^{\mathcal{E}}\right] & \frac{1}{\mathbf{C}^{\mathcal{N}}}\left[-\mathbf{G}^{cte}\right] & 0 \\ -\mathcal{L}2\boldsymbol{\alpha} & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^c \end{bmatrix} \tag{3.1}$$

The above system formulation is represented in state space form $\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$ based on the system's co-energy variables $\mathbf{I}^{\mathcal{G}}$, $\mathbf{I}^{\mathcal{E}}$, $V^{\mathcal{N}}$ and $\boldsymbol{\eta}^c = \mathbf{K}_I\mathbf{x}_c$. In order to achieve a pH formulation of the interconnected microgrid, the above system representation needs to be remodelled with respect to the system energy variables written as functions of the co-energy variables. The autonomous linear system is then presented as the time derivative of the energy variables $\boldsymbol{\phi}$, $\mathbf{q}$ and $\mathbf{x}_c$ instead of the time derivative of the co-energy variables $\mathbf{I}$, $\mathbf{V}$ and $\boldsymbol{\eta}$. In order to achieve a fully skew-symmetric dynamical $\mathbf{A}$-matrix, the $\mathbf{K}_I$-term containing the integral gains of the controllers, are rather implemented after the integration of the cyber states. Hence, the energy variables of the control network will be $\mathbf{x}_c$ and the co-energy variable is now defined as $\boldsymbol{\eta}^c = \mathbf{K}_I\bar{\mathbf{x}}_c$. With this change in the control system, multiplying the integral gain after the state integration, the pH system representation of the cyber layer is now expressed as:

$$\sum_c : \begin{cases} \dot{\mathbf{x}}_c = \mathbf{g}_c\mathbf{u}_c = -\mathcal{L}\mathbf{u}_c \\ \mathbf{y}_c = \mathbf{g}_c^\top \boldsymbol{\nabla} H_c(x_c) = -\mathcal{L}\mathbf{K}_I\mathbf{x}_c \end{cases} \tag{3.2}$$

The final state space representation of the MG, based on the pH formalism, is presented below with the associated energy variables. This representation emphasizes the energy of the system by presenting the skew-symmetric properties: i.e., the power is preserved within the system which is proven important for the stability of the system when using Lyapunov's method. In order to present the system on the pH form exploiting the relations between the energy and co-energy variables, the final representation in 3.1 is re-written. The relation between the co-energy and energy variables are expresses in the quadratic matrix $\mathbf{Q}$ defined in the associated specialization project as a generalized inertia matrix. The quadratic matrix is defined as:

$$\mathbf{Q} = \begin{bmatrix} \frac{1}{\mathbf{L}^{\mathcal{G}}} & 0 & 0 & 0 \\ 0 & \frac{1}{\mathbf{L}^{\mathcal{E}}} & 0 & 0 \\ 0 & 0 & \frac{1}{\mathbf{C}^{\mathcal{G}}} & 0 \\ 0 & 0 & 0 & \mathbf{K}_I \end{bmatrix}$$

In order to re-write the system in compact form based on both energy and co-energy variables the inverse $\mathbf{Q}$-matrix is multiplied in each term: $\mathbf{Q}^{-1}\dot{\mathbf{x}} = \mathbf{Q}^{-1}\mathbf{A}\mathbf{x}$, where

$$\mathbf{Q}^{-1} = \begin{bmatrix} \mathbf{L}^{\mathcal{G}} & 0 & 0 & 0 \\ 0 & \mathbf{L}^{\mathcal{E}} & 0 & 0 \\ 0 & 0 & \mathbf{C}^{\mathcal{G}} & 0 \\ 0 & 0 & 0 & \frac{1}{\mathbf{K}_I} \end{bmatrix}$$

The final pH system is now presented below, emphasizing the skew-symmetry: i.e., the algebraic representation of power preservation of the interconnected system.

$$\begin{bmatrix} \dot{\boldsymbol{\phi}}^{\mathcal{G}} \\ \dot{\boldsymbol{\phi}}^{\mathcal{E}} \\ \dot{\mathbf{q}}^{\mathcal{N}} \\ \dot{\mathbf{x}}^c \end{bmatrix} = \begin{bmatrix} \left[2\boldsymbol{\alpha}(-K_p\mathcal{L}2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \left[-\mathcal{B}^{\mathcal{G}\top}\right] & \left[2\boldsymbol{\alpha}\mathcal{L}\right] \\ 0 & \left[-\mathbf{R}^{\mathcal{E}}\right] & \left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \left[\mathcal{B}^{\mathcal{G}}\right] & \left[\mathcal{B}^{\mathcal{E}}\right] & \left[-\mathbf{G}^{cte}\right] & 0 \\ \left[-\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^c \end{bmatrix} \tag{3.3}$$

The closed loop control system associated to the above linear representation, is then presented below. The proposed passivity based PI-controller, $\mathbf{r}$, is implemented when closing the control loop giving the final secondary control system:

$$\begin{aligned} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} &= \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^\top & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} & -(2\boldsymbol{\alpha}) \\ (2\boldsymbol{\alpha})^\top & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ \boldsymbol{\beta} \end{bmatrix} \end{aligned} \tag{3.4}$$

When studying the intrinsic dynamics of the closed loop control system, the skew-symmetric properties are recognized and the relations between the control outputs and inputs are then defined as below. $\mathbf{F}_L \in \mathbb{R}^{2\times 2}$ is

the lossy interconnection matrix containing the added controller, $\mathbf{r}$, and added weightings $\mathbf{w}^{-1}$.

$$\begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} = \mathbf{F}_L \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} \tag{3.5}$$

When considering the power flow between the two systems$\mathbf{uy}$ is equals transferred power. As the interconnection of the two networks are presumed power preserving for the unforced system, the control system may be expressed as:

$$-\begin{bmatrix} \mathbf{y}_{tot} & \mathbf{y}_c \end{bmatrix} \mathbf{F}_T^{\top} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} = 0 \tag{3.6}$$

From the above representation, and the definition of skew-symmetry, it is valid to say that the input and output terms will cancel each other out by $\mathbf{y}_{tot} = \mathbf{u}_c$ and $\mathbf{u}_{tot} = -\mathbf{y}_c$ representing power preservation.

With the above closed loop control system, the passivity based secondary controller is expressed in scalar form below presenting the optimal system representation when no cyber attacks are perturbing the MG.

$$\begin{cases} u_{tot} = R_i^D I_i^{\mathcal{G}} + 2\alpha_i(K_p z_i^{\lambda} - z_i^c) \\ \dot{x}_i^c = z_i^{\lambda} \\ z_i^{\lambda} = \sum_{j \in \mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) \\ z_i^c = \sum_{j \in \mathcal{N}_c} a_{ij} K_i^I (x_j^c - x_i^c) \\ \lambda_i = 2\alpha_i I_i^{\mathcal{G}} + \beta_i \end{cases} \tag{3.7}$$

# 4 Approach to Analyse Cyber Attacks and Resilience

In the following sections three types of cyber attacks are studied. The intention of the cyber attack analyses is to present the cyber attack construction approach for the linear cyber-physical MG, assess the drawbacks entailed by the different attacks, and investigate if the proposed resilient controller is robust enough when the attacks are intruding. The three cyber attacks studied are *false data injected into the actuators of the secondary controller*, *false data added to the current sensors in the DGs* and *man-in-the-middle attack intruding in the communication links of the cyber layer*. They are chosen as the studied cyber attacks as they perturb in different locations of the MG dynamics: one in the interconnections between the two sub-systems and one in each of the two layers. The three attacks will therefore potentially malign the control objectives in different ways and *if* this thesis achieves to model a resilient controller robust against all these three attacks, it is then concluded that the controller is novel. In other words, the controller is able to ensure resilience against all cyber attacks regardless of where the attacks perturb.

The following approach is used to analyse the system: The cyber attack is first modelled in the linear state-space representation of the MG dynamics, establishing the perturbed system of study. A stability analysis is then conducted in order to validate if the system converges to a steady state equilibrium while being under attack. Then the two control objectives are studied at the potential new equilibrium point of the perturbed system. The resilience of the controller is then studied: i.e., assessing if the two control objectives are ensured while the primary control parameter $\boldsymbol{\alpha}$ is tuned to a significant high value, defined by the bound of the attack. The perturbed system is then simulated for a case specific MG with arbitrary attack values. The performance of the resilient control strategy is then tested by tuning the control parameter to the defined significant resilience value. The simulations are used to support the obtained mathematical proofs.

# 5 Cyber Attack 1: Attacking in the Actuators of the Control System

The first studied cyber attack infiltrates in the actuators of the secondary controller. The potential attack is modelled as a false data injection attack, perturbing the control system with external input due to the on-line communication links in the cyber layer. The attack vector, $\Delta\mathbf{u}$ is adding values on top of the secondary controller delivered to the physical layer: i.e., the attack is disturbing in the interconnections between the physical network and cyber network. Figure 5.1 visualizes–from an energy control (pH) perspective–how the attack vector infiltrates the control interconnections, adding values on top of the secondary control inputs. As the attack is perturbing the control actions of the physical network it is assumed to affect the controllers ability to ensure average voltage regulations, and the secondary controller's ability to restore the initial conditions where $\mathbf{V} = 48V$ are assumed weakened.

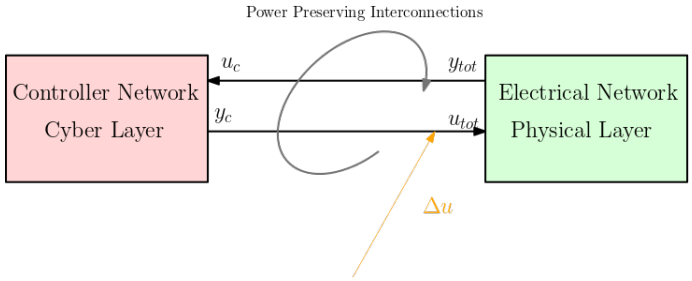


Figure 5.1: pH representation of closed loop control system subject cyber attacks in the control actuators

## 5.1 Cyber Attack Modelling

In order to later assess the perturbed system with respect to its stability and ability so ensure optimal performance, the attack vector needs to be constructed with respect to the inherent dynamics of the cyber-physical MG. The DC MG studied in this thesis admits the pH formalism and the state space model is expressed with associated energy and co-energy variables. The state space model of the closed loop linear dynamics is now modified in order to include the external input: i.e., the attack vector $\Delta\mathbf{u}$. The input matrix $\mathbf{B}$ contains the attack infiltration dynamics: i.e., the necessary dynamics in order to infiltrate the power system at the desired location. As the cyber attack of study is adding values on top of the secondary control of the DGs, the attack is directly entering the dynamics of the generators. For the case specific MG, modelled with four generating units, the input matrix $\mathbf{B}$ will only contain elements with respect to the generators and $\mathbf{1}_4$ is defined as a $(4 \times 4)$ Identity matrix.

$$\begin{bmatrix} \dot{\boldsymbol{\phi}}^{\mathcal{G}} \\ \dot{\boldsymbol{\phi}}^{\mathcal{E}} \\ \dot{\mathbf{q}}^{\mathcal{N}} \\ \dot{\mathbf{x}}^{c} \end{bmatrix} = \begin{bmatrix} \left[2\boldsymbol{\alpha}(-K_p\mathcal{L}2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \left[-\mathcal{B}^{\mathcal{G}\top}\right] & [2\boldsymbol{\alpha}\mathcal{L}] \\ 0 & \left[-\mathbf{R}^{\mathcal{E}}\right] & \left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \left[\mathcal{B}^{\mathcal{G}}\right] & \left[\mathcal{B}^{\mathcal{E}}\right] & \left[-\mathbf{G}^{cte}\right] & 0 \\ -\left[\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^{c} \end{bmatrix} + \begin{bmatrix} \mathbf{1}_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta\mathbf{u} \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{5.1}$$

**Closed Loop Control System**

The final control system is then modified to include the cyber attack. The closed loop control system is then expressed below with only one additional matrix containing the added false values in regards to the secondary controller $\mathbf{u}_{tot}$.

$$\begin{aligned} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} &= \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \begin{bmatrix} \Delta\mathbf{u} \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} & -(2\boldsymbol{\alpha}) \\ (2\boldsymbol{\alpha})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ \boldsymbol{\beta} \end{bmatrix} + \begin{bmatrix} \Delta\mathbf{u} \\ 0 \end{bmatrix} \end{aligned} \tag{5.2}$$

With the above closed control network and added attack vector, the dynamics of the secondary controller is

expressed below.

$$\begin{cases} u_{tot} = R_i^D I_i^{\mathcal{G}} + 2\alpha_i(K_p z_i^{\lambda} - z_i^c) + \Delta u_i \\ \qquad = R_i^D I_i^{\mathcal{G}} + 2\alpha(-K_p \mathcal{L}\lambda + K_i^I \mathcal{L} x_i^c)\Delta u_i \\ \dot{x}_i^c = z_i^{\lambda} \\ z_i^{\lambda} = \sum_{j\in\mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) \\ z_i^c = \sum_{j\in\mathcal{N}_c} a_{ij} K_i^I (x_j^c - x_i^c) \\ \lambda_i = 2\alpha_i I_i^{\mathcal{G}} + \beta_i \end{cases} \tag{5.3}$$

All the dynamics of the MG are now modified to be subject to FDI attacks in the actuators of the controller. The perturbed CP MG can then be asses with respect to the bounded stability and the resilience is lastly tested.

## 5.2 Energy Flow Analysis

As the attack is perturbing in the connections between the cyber layer and the physical layer, this section assesses how the cyber attack changes the power flows between the two network:s i.e., disturbing the power preserving interconnections.

$$\begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} = \mathbf{F}_L \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \begin{bmatrix} \Delta\mathbf{u} \\ 0 \end{bmatrix} \tag{5.4}$$

When the control network are of of closed loop with added attack vectors, it is shown above that the power preserving interconnections between the input-and output ports have been compromised. $\mathbf{F}_L$ represent the lossy interconnection matrix containing the weighted power preserving interconnections with the added dissipation, $\mathbf{r}$, between $\mathbf{u}_{tot}$ and $\mathbf{y}_c$. The secondary controller is then described as a function of the associated port-variables and the added attack: $\mathbf{u}_{tot} = -\mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{b} + \Delta\mathbf{u}$. As the attack is perturbing in the energy transfer from the cyber layer to the physical layer, the cyber controller input remains unchanged compared to the unforced case: $\mathbf{u}_c = \mathbf{w}^{-1^\top}\mathbf{y}_{tot} + \mathbf{b}_c$. However, it is assumed that the cyber controller also is perturbed as it is a function of the output values of the disturbed electrical network.

### 5.2.1 Power Flows

Before studying the closed loop in detail, the flow of the stored (physical and virtual) energy of the MG is assessed. The Hamiltonian, $H_T(x_T)$ is firstly defined for the open loop system as the sum of the two syb-systems individual stored energy. In the electrical pH system representation defined 1.13 in *Part A*, it is defined that the time derivative of the generator states in the electrical system are linearly affected by the secondary control input, $\mathbf{u}_{tot}$, which is now the attacked term. Hence, the change in electric energy with respect to time will also depend on the secondary controller and therefore change with respect to the potential attack in the actuators of the controller. However, the time invariant stored energy of both the cyber layer and physical layer will be defined as:

$$\begin{aligned} H_T(x_T) &= H_{tot}(x_{tot}) + H_c(x_c) \\ &= \frac{1}{2}\mathbf{x}_{tot}^\top \mathbf{Q}_{tot}\mathbf{x}_{tot} + \frac{1}{2}\mathbf{x}_c^\top \mathbf{K}_I \mathbf{x}_c \end{aligned} \tag{5.5}$$

$H_T$ is the stored energy of the CP MG: i.e., the Hamiltonian, $H_{tot}$ is the stored energy of the electrical system and $H_c$ is the stored cyber energy related to the PI integrator state in the cyber layer. The time-dependent energy functions are obtained by using the chain rule on the sub-systems individual Hamiltonians. The chain rule is expressed below, and the time-dependent energy functions are defined as the energy output multiplied with the individual systems states.

$$\dot{H}(x) = \frac{d}{dt}H(x) = \frac{\partial H}{\partial x}\cdot\frac{\partial x}{\partial t} = \frac{\partial}{\partial x}H(x)\cdot\dot{x} = \nabla^\top H(x)\cdot\dot{x}$$

The states regarding the electrical energy, $\dot{\mathbf{x}}_{tot}$, and cyber states, $\dot{\mathbf{x}}_c$, are given in 1.13 and 3.2 respectively defined in *Part A*. $\dot{H}_T(x_T)$ is then expressed below by using the chain rule and added energy of each dynamic term.

$$\begin{aligned} \dot{H}_T(x_T) &= \dot{H}_{tot}(x_{tot}) + \dot{H}_c(x_c) \\ &= \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{F}_{tot}\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot}^{\mathcal{G}} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c \end{aligned} \tag{5.6}$$

The stored energy of the separate sub-systems are now established and the energy change of the interconnected MG may be further assessed when closing the control loop. Towards this end, the power preserving interconnections are then used to express the control parameters as a function of the associated port variables as done in *Part B* Section 5.2. The intention is to see if some terms of the time derived Hamiltonian are cancelling out due to power preservation. The final function describing the energy changes of the closed loop MG is then expressed only by the terms contributing with added and/or reduced energy due to the attack and inherent dissipation. This function may then be used as a starting point to analyse the stability of the system, as a power system with constantly increasing energy will become unstable. In 3.2 the change in cyber energy is defined as the transposed output value of the cyber layer multiplying the received input value. The last term of the time-dependent Hamiltonian is therefore expressed as:

$$\begin{aligned}\boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c &= \mathbf{y}_c^\top \mathbf{u}_c \\ &= \mathbf{y}_c^\top(\mathbf{w}^{-1^\top}\mathbf{y}_{tot} + \mathbf{b}_c) \\ &= \mathbf{y}_c^\top \mathbf{w}^{-1^\top}\mathbf{y}_{tot} + \mathbf{y}_c^\top \mathbf{b}_c \end{aligned} \tag{5.7}$$

Equally the energy change of the electrical network, $\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}$ is defined in 1.13 in *Part A* as the transposed output value of the physical layer, $\mathbf{y}_{tot}$, multiplied with the received input value acquired from the connecting cyber layer. Using the transferred energy as the input/output values and the skew-symmetric properties defined in 5.2 the second term of $\dot{H}_T(x_T)$ is represented below.

$$\begin{aligned}\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} &= \mathbf{y}_{tot}^\top \mathbf{u}_{tot} \\ &= \mathbf{y}_{tot}^\top(-\mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{b} + \Delta\mathbf{u}) \\ &= -\mathbf{y}_{tot}^\top \mathbf{r}\mathbf{y}_{tot} - \mathbf{y}_{tot}^\top \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_{tot}^\top \mathbf{b} + \mathbf{y}_{tot}^\top \Delta\mathbf{u} \end{aligned} \tag{5.8}$$

The final expression describing the energy changes of the closed loop interconnected MG is expressed in 5.9. The controller parameter $\mathbf{r}$, defined in 5.8, is added to the dissipation matrix $\mathbf{R}_T$ with respect to the states of the electrical network constituting the new dissipation matrix $\mathbf{T}_T$. This is due to the fact that the control network is interconnected through the generators: i.e., states of the electrical network. The first term of $\dot{H}_T$ is then adjusted so that $\mathbf{F}_{tot} = (\mathbf{J}_{tot} - \mathbf{T}_T)$ and the matrices $\mathbf{R}^{\mathcal{G}}$, $\mathbf{R}^{\mathcal{D}}$, $\mathbf{R}^{\mathcal{E}}$ and $\mathbf{G}_{cte}^{\mathcal{N}}$ are positive definite as the impedance always is $\geq 0$. Hence, $\mathbf{T}_T$ is positive definite as $\mathbf{r}$ also is defined positive definite. $\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{J}_{tot}\boldsymbol{\nabla}H_{tot}(x_{tot})$ is equal to power conservation and the term is therefore equal to zero in regards to time dependence. The first term is therefore modified to $-\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot})$ representing the power dissipation of the closed loop microgrid.

By using the mathematical relation of transposed matrices, two terms of the sub-system energy functions will cancel out as $\mathbf{y}_c^\top \mathbf{w}^{-1^\top}\mathbf{y}_{tot} - \mathbf{y}_{tot}^\top \mathbf{w}^{-1}\mathbf{y}_c = 0$. It is therefore shown that the term related to the added cyber energy flow will cancel out the energy dissipation of the electrical network in the interconnections, achieving power preservation in some parts of the interconnected MG. However, the term related to the attack is not being cancelled out and the final change in energy is expressed as:

$$\begin{aligned}\dot{H}_T(x_T) &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) + \mathbf{y}_{tot}^\top \mathbf{b} + \mathbf{y}_{tot}^\top \Delta\mathbf{u} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \mathbf{y}_c^\top \mathbf{b}_c \\ &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})(\mathbf{b} + \Delta\mathbf{u}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{b}_c \end{aligned} \tag{5.9}$$

## 5.3 Stability Analysis

The primary stability assessment method used in this thesis, is the Lyapunov stability theorem aiming to establish a generalized stability proof, valid for both linear and nonlinear systems. The Lyapunov's method assesses the stability without needing to obtain the time response of the system avoiding integrating the system states and the stability is not evaluated based on locating the eigenvalues. In addition small system stability approaches using the eigenvalues require the initial conditions of the system in order to acquire the integrated values. The stability conclusion will therefore be highly dependent on the starting conditions of the system. The Lyapunov's method is rather based on assessing the energy functions, avoiding integration and establishing a valid stability certificate regardless of the initial staring point of the energy functions. The conducted stability certificate is therefore generalized, global and valid for linear and nonlinear system independent of the starting point. In order to preform this Lyapunov stability analysis, the change in energy firstly needs to be based on incremental energy.

### 5.3.1 Incremental Energy Modelling

The incremental model assumes that the closed loop MG has an unique equilibrium point. This is previously expressed in *Assumption* 1, as an assumption necessary when preforming all system analyses in this thesis. Hence, it is assumed that both the electrical network and the control network has individual unique equilibrium points. The incremental energy model is then defined from the energy difference between the energy at the system operational state and the energy at the desired equilibrium. The incremental states are expressed as $\tilde{\mathbf{x}} = \mathbf{x} - \bar{\mathbf{x}}$ where $\bar{\mathbf{x}}$ represent the states at the optimal equilibrium and $\mathbf{x}$ is the operational present studied states. The constants of the system appears in both the operational state and the desired equilibrium, and are therefore cancelled out when incremental energy terms are assessed. The expression for the incremental states of the closed loop MG, $\sum_T$, are presented below.

$$\begin{aligned}
\dot{\mathbf{x}}_T &= (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(x_{tot}) + \mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} + \mathbf{E}_{tot} + \mathbf{g}_c\mathbf{u}_c \\
-\ 0 &= (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(\bar{\mathbf{x}}_{tot}) + \mathbf{g}_i^{\mathcal{G}}\bar{\mathbf{u}}_{tot} + \mathbf{E}_{tot} + \mathbf{g}_c\bar{\mathbf{u}}_c \\
\hline
(\dot{\mathbf{x}}_T - 0) &= (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(x_{tot} - \bar{\mathbf{x}}_{tot}) + \mathbf{g}_i^{\mathcal{G}}(\mathbf{u}_{tot} - \bar{\mathbf{u}}_{tot}) + \mathbf{g}_c(\mathbf{u}_c - \bar{\mathbf{u}}_c) \\
\dot{\tilde{x}}_T &= (\mathbf{J}_{tot} - \mathbf{R}_{tot})\boldsymbol{\nabla} H_{tot}(\tilde{x}_{tot}) + \mathbf{g}_i^{\mathcal{G}}\tilde{\mathbf{u}}_{tot} + \mathbf{g}_c\tilde{\mathbf{u}}_c
\end{aligned} \tag{5.10}$$

The time-dependent Hamiltonian of the closed loop system, based on incremental energy, is then defined in 5.11. Clearly, all the terms related to the constant inputs ($\mathbf{E}_{tot}$, $\mathbf{b}$, $\mathbf{b}_c$) are disappearing. The term related to the attack will not disappear when the attacks are defined as a time varying intrusions. In order to establish a proof valid for both constant and time varying cyber attacks, $\Delta\mathbf{u}$ is represented as an incremental attack vector: i.e., with different values $\Delta\bar{\mathbf{u}} \neq \Delta\mathbf{u}$. With this energy model the time-dependent incremental energy function is expressed as:

$$\dot{H}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla} H_{tot}(\tilde{x}_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\Delta\tilde{\mathbf{u}} \tag{5.11}$$

### 5.3.2 Lyapunov Stability Certificate

The next part of the stability analysis is the final assessment of whether the control system is able to ensure steady state operations while being under cyber attack 1: i.e., finding a valid stability certificate with the included perturbation term. The stability proof is based on proposing a storage function named a Lyapunov candidate, $V(x)$, and assess the time-dependent changing Lyapunov function. The proposed storage function is based on the function describing the incremental energy changes of the closed loop system, given in 5.11. Incremental energy is beneficial as the time-dependent Lyapunov function now is required to have a minimum at the point of interest. It is then possible to assess how the incremental energy changes and potentially ascertain that the closed loop MG will converge to the steady state equilibrium.

As the system of study now is modelled as a perturbed system, and due to *Assumption* 3 and *Assumption* 1, this section uses Lyapunov stability to show the system is exponential stable at the system equilibrium for a given bound of the states, enforced by the uniformly bounded attack. Using *Lemma 4.5* in Nonlinear control [23] the stability may be concluded by first assessing the stability of the unforced system. The theorem states that if the unforced system is achieving exponential stability, then the perturbed system is *input - to - state stable* (ISS) and, because the system is also linear it is achieving the *bounded input - bounded state* (BIBS) property. The first step is then to establish a positive definite Lyapunov function candidate of the unforced system, having a minimum at the equilibrium point of interest and show that the time-derivative of this storage function will be negative semidefinite when the attack is ignored. First, the stored incremental energy of the total MG is expressed as a sum of the sub-system's stored energy with respect to the incremental states. The Lyapunov candidate is proposed as:

$$\begin{aligned}
V_T(\tilde{x}_T) &= H_{tot}(\tilde{x}_{tot}) + H_c(\tilde{x}_c) \\
&= \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top\mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top\mathbf{K}_I\tilde{\mathbf{x}}_c
\end{aligned} \tag{5.12}$$

The time-derivative of the Lyapunov candidate $\dot{V}(\tilde{x}_T)$ of the perturbed system is then ascertained as a function inspired by the closed loop energy function given in the previous section. The final expression for the time-derivative of the Lyapunov candidate is then specified below.

$$\begin{aligned}
\dot{V}_T(\tilde{x}_T) &= \dot{H}_{tot}(\tilde{x}_{tot}) + \dot{H}_c(\tilde{x}_c) \\
&= -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla} H_{tot}(\tilde{x}_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\Delta\tilde{\mathbf{u}}
\end{aligned} \tag{5.13}$$

The two energy functions are then assessed with respect to Lyapunov's global stability criteria, concluded when $V(\tilde{x}) > 0, V(\bar{x}) = 0, \dot{V}(\tilde{x}) \leq 0$ and $\dot{V}(\bar{x}) = 0$. The Lyapunov theorem states that *the orgin is stable if, in a domain D that contains the orgin, there is a continuous differential positive definite function* $V(x)$ *so that* $\dot{V}(\mathbf{x})$ *is negative semidefinite and it is asymptotically stable if* $\dot{V}(x)$ *is negative definite* [25]. The positive/ negative *definite* and *semidefinite* definitions are given in the associated specialization project.

The first global stability criteria states that the the Lyapunov function of the autonomous linear system needs to be a scalar storage function $V(\tilde{x})$ as proven valid for the proposed functions above. This is due to the fact that $\tilde{\mathbf{x}}^\top \mathbf{Q} \tilde{\mathbf{x}}$ is equal to the summation of all the states as $\mathbf{Q}$ and $\mathbf{K}_I$ are quadratic matrices of the necessary dimensions. $V(\tilde{x})$ is then specified as the continuous differential function defined in a domain $\mathbb{D} \subset \mathbb{R}^n$ containing the initial operating point [25]. The scalar Lyapunov function is proven positive definite, $V_T(\tilde{x}_T) > 0$ as energy is always preserved. The second global stability criteria, $V(\bar{x}_T) = 0$, is proven valid as $\bar{x}_T$ always represents the state variables bringing the energy to zero: i.e., achieving steady state at the equilibrium point. The proposed storage function $V(\tilde{x})$, containing the conserved quantities, is defined as a dissipated quantity if $\dot{V}(\tilde{x}_T)$ is non-increasing which respect to time. This is desirable as the stability may only be concluded if the energy is not increasing towards infinity. $\dot{V}(\tilde{x}_T)$ is expressed as function of the energy dissipation as explained when $\dot{H}(x_T)$ where obtained, when disregarding the attack. The Lyapunov candidate is therefore defined negative semidefinite, presenting a function decreasing along the trajectories of the autonomous system passing through the state $\bar{x}$ bringing the system to stable conditions [25]. Hence, the energy analysis corresponds to assessing if system is stabilizing at an assignable equilibrium point. In order to conclude global stability the change in energy at the equilibrium point needs to be assessed. $\dot{V}(\bar{x}_T) = 0$ is only valid when $\mathbf{x} = \bar{\mathbf{x}}$ and the system is proven to achieve stability at the minimum value of interest i.e converging to the steady state equilibrium.

$\dot{V}(\tilde{x}_T) < 0$ is the additional citeria that needs to be satisfied to conclude on global and asymptotic stability. La Salle's argument is applied in order to ensure asymptotic stability by assessing the state variables at the system minimum: i.e., assessing the equation $\dot{V}_T(\tilde{x}_T) = 0$. $\mathbf{T}_T$ is of full rank, $\mathbf{Q}_{tot}$ is quadratic, and $\dot{V}_T(\tilde{x}_T)$ is then equal to zero if the state variables, $\tilde{\mathbf{x}}_{tot}$, is zero. The incremental states are equal to zero when $\mathbf{x}_{tot} = \bar{\mathbf{x}}_{tot}$ and it is proven that the minimum of the Lyapunov function equals the equilibrium point of interest $\bar{\mathbf{x}}_T$. Thus, it is proven that the closed loop MG, based on the incremental energy, achieves global asymptotic stability (GAS) when disregarding the perturbation term.

### 5.3.3 Input- to - state stability

In the above analysis it is proven that the unforced system is asymptotically converging to a global equilibrium point. This is proven valid for the case specific linear autonomous system and it is therefore equally valid to conclude that the system converges globally and exponentially to the equilibrium due to the linear dynamics [23]. Invoking *lemma 4.5* from Nonlinear control [23] the perturbed system–subject to cyber attacks in the actuators–is ISS as the unforced system is exponentially stable. This means that the system is stable with respect to a given bound of the states. The bound is entailed by the bounded attack and the system achieves the BIBS property.

### 5.3.4 Interpretation of the Lyapunov Input - to - State Stability

When the cyber attack is infiltrating the actuators of the controller, it is not possible to conclude on global asymptotic stability due to the added perturbation term. However, it is possible to conclude that the energy of the system always converges to a bounded periphery containing the new equilibrium, regardless of the starting point. It is therefore valid to declare that the system is *input - to - state* stable as the energy function converges to a new equilibrium within the bound, that is the closest possible equilibrium in regards to the desired equilibrium. Without loss of generality we will be treating the attacks as constants in steady-state, since if this is not the case and it is instead time-varying at the equilibrium, we can still bound the energy function by a constant specified by the bound of the attack.

When ISS is concluded it is then feasible to assess the boundedness of the attack vector for the linear system: i.e., obtaining the value of the bounded periphery. A potential further study is then to research how to reduce the bound so that the system always converges to the actually desired equilibrium.

## 5.4 Obtaining the Bound of the Attack

The Lyapunov's method is so far used to form a Lyapunov candidate $V(x)$ that is positive definite in the domain $D \subset \mathbb{R}^n$ and $\dot{V}(x)$ is negative definite in $D$ so we can conclude on global asymptotic stability. This section shows how Lyapunov's method additionally may be used to express the stability bound entailed by the external cyber attack. In other words, when the *input - to - state* stability is ensured, then the Lyapunov theory may be used to express the value of the restrictive stability bound of the states. The applied approach is equal to the approach presented in *Appendix* E when obtaining the *region of attraction* for a unforced system. However, the approach aims to obtain the opposite to the *region of attraction*: i.e., the intention is to establish the upper bound of the stable states. The perturbed system is ensured to always achieve global uniformly asymptotic stability when the states are defined for a value less than that bound defined by uniformly bounded perturbation term. Subsequently, the expression of the final bound is presented.

**Radially Unbounded**
In this thesis, the proposed Lyapunov function is given as the quadratic function $V(\tilde{x}) = \tilde{x}^\top P\tilde{x}$ defined for a certain neighbourhood of the orgin with respect to incremental energy. Due to the quadratic property, the Lyapunov function is certified *radially unbounded* meaning that the function of the perturbed system $f(x, u)$ is a continuous differentiable function defined over $D$, where $D = \mathbb{R}^{n^{\mathcal{G}}+n^{\mathcal{E}}+n^{\mathcal{N}}}$. Using the *Variable gradient method* where $x^\top Px \geq \lambda_{min}(P) \parallel x \parallel^2$ it is defined that if $x^\top Px$ is positive definite, then the Lyapunov function is *radially unbounded*. The domain $D$ is then equal to the region of attraction. The radial unboundedness is used, in regards to the Lyapunov theorem, to ensure that the orgin is globally uniformly asymptotically stable by expressing that the set $\Omega_c = \{V(x) < c\}$ is bounded for every $c > 0$. Without this condition the set $\Omega_c$ might not be bounded for large $c$ and globally asymptotic stability is not ensured.

**Boundedness of the Cyber Attack in the Control Actuators**
The last part of this section aims to use the presented definition of *radially unboundedness* in order to express the bounded value of the steady state stability, restricted by the cyber attacks. The Lyapunov function is defined as radially unbounded due to the qudratic properties of $\mathbf{Q}_{tot} \in \mathbb{R}^{n\times n}$ and $\mathbf{K}_I \in \mathbb{R}^{n\times n}$ and the obtained region of attraction is specified with respect to the cyber attack. We are therefore interested in obtaining the bound of the states restricted by $c > 0$ where $c$ is identified as largest cyber attack bound on which $\dot{V}(x)$ is proven negative definite. Figure 5.2 presents a simple visualization of the BIBS property where the Lyapunov functions are shows to always converge to the periphery of the bounded set $\mathbf{B}_r$.

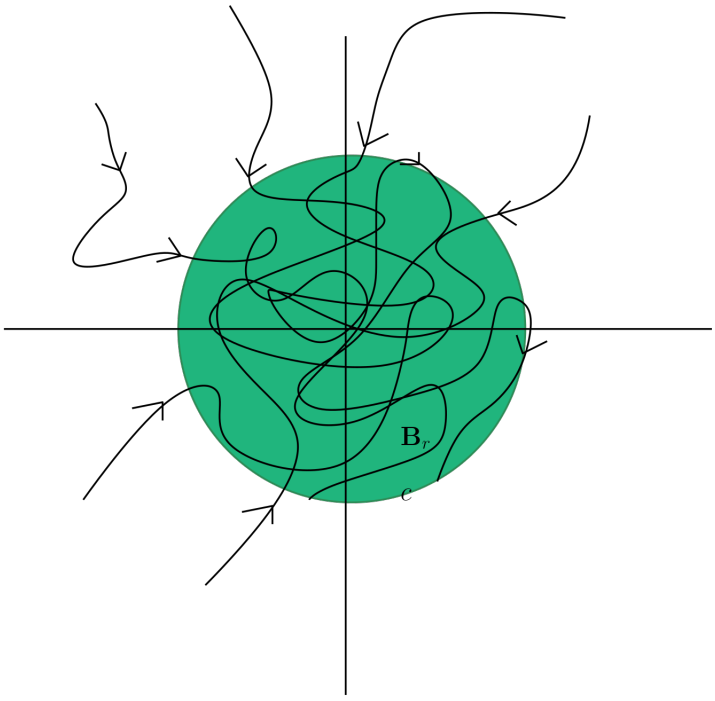


Figure 5.2: Bounded Input Bounded State

*Theorem 4.1* and *Theorem 4.2* in Khalil's Nonlinear Control is then applied [23]. If the parameters $r$ and $c$ are chosen such that the bound of the states are expressed as $\mathbf{B}_r = \{\parallel \mathbf{x} \parallel \leq r\} \subset D$ and $c < \lambda_{min}(P)r^2$, then

the derivative along the trajectories of the Lyapunov function is expressed as:

$$\dot{V}_T(\tilde{x}_T) = -\tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot}\mathbf{T}_T\mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot}\mathbf{g}_i^{\mathcal{G}}\Delta\tilde{\mathbf{u}} \tag{5.14}$$

$$\leq -\lambda_{min}(\mathbf{T}_T) \parallel \mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} \parallel^2 + \parallel \tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot}\mathbf{g}_i^{\mathcal{G}}\Delta\tilde{\mathbf{u}} \parallel \tag{5.15}$$

$$\leq -\lambda_{min}(\mathbf{T}_T) \parallel \mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} \parallel^2 + \parallel \tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot} \parallel\parallel \mathbf{g}_i^{\mathcal{G}}\Delta\tilde{\mathbf{u}} \parallel \tag{5.16}$$

$\lambda_{min}$ is the minimum eigenvalue of the symmetric matrix $\mathbf{T}_T$. The system is proven globally uniformly asymptotically stable when $\dot{V}_T(\tilde{x}_T) \leq 0$. The equation above is then solved with respect to the states, in order to express the bound that satisfied the global uniformly asymptotic stability criteria. The final bound of the states are expressed below and the BIBS property is certified for a specific value of the bounded attack.

$$\parallel \mathbf{Q}\tilde{\mathbf{x}}_{tot} \parallel \geq \frac{\parallel \mathbf{g}_i^{\mathcal{G}}\Delta\tilde{\mathbf{u}} \parallel}{\lambda_{min}(\mathbf{T}_T)} \tag{5.17}$$

The deduction of the bounded states are, for this cyber attack in the control actuators, simple to express as the attack is only perturbing with respect to the physical states. However, if the final Lyapunov function presents its stability where the attack bounds both the physical states, $\tilde{\mathbf{x}}_{tot}$, and the cyber states, $\tilde{\mathbf{x}}_c$, then the attack brings two different bounds to the system complicating the deduction of the bound. This is the case for the next studied cyber attacks and the bound is therefore only expressed mathematically for this first studied cyber attack.

## 5.5 Equilibrium Analysis

Given *Assumption* 1 it is assumed that the interconnected network has one unique equilibrium point as the two sub-network both converges to individual equilibrium points. This assumption is still valid as the above section proves that the system achieves input-to state stability at a new equilibrium point while the system is under cyber attack in the actuators of the controller. The next step is then to assess if the proposed secondary controller still is able to ensure that the two main control objectives, equal incremental costs and average voltage regulation, are satisfied at the new equilibrium point. The intention of the proof below is then to assess the control performance at the steady state equilibrium and evaluate the properties of the microgrid under the new control conditions.

The equilibrium point of the distributed control network is firstly assessed at steady state: i.e, when the time derivative of the cyber controller states equals zero. Combining the defined control network in 3.2 and the controller in *Definition* 1, the cyber states are expressed as: $\dot{\mathbf{x}}_c = \mathbf{z}^\lambda = -\mathcal{L}\boldsymbol{\lambda} = -\mathcal{L}(2\boldsymbol{\alpha}\mathbf{I} + \boldsymbol{\beta})$. The steady state equilibrium of the cyber layer are then presented as:

$$0 = -\mathcal{L}(2\boldsymbol{\alpha}\bar{\mathbf{I}} + \boldsymbol{\beta}) \tag{5.18}$$

The above equation will be valid when $(2\boldsymbol{\alpha}\bar{\mathbf{I}} + \boldsymbol{\beta}) = \mathbf{1}\lambda_{opt} = \bar{\boldsymbol{\lambda}}$ due to the Laplacian property where $\mathcal{L}\mathbf{1} = 0$. $\bar{\boldsymbol{\lambda}}$ is the optimal consensus value of the incremental costs, at the converged equilibrium. The equilibrium of the forced control network is therefore shown to satisfy the control objective *1.* All the DGs needs to agree upon one optimal consensus value of the incremental costs in order to satisfy the indicated steady state of the network. It is also recognized in the equation above that the proposed resilient controller in *Hypothesis* 1 will not affect the ability to ensure consensus. For this perturbed system the consensus is always ensured due to the Laplacian, regardless of the tuning of $\boldsymbol{\alpha}$.

The equilibrium of the closed loop network is then assessed by studying the controllers presented in *Part B* Section 5.2 at the new converged equilibrium point identified due to the attack:

$$\begin{aligned}\bar{\mathbf{u}}_{tot} &= \mathbf{R}^D\bar{\mathbf{y}}_{tot} + 2\boldsymbol{\alpha}(K_p\mathbf{z}^\lambda - \mathbf{z}^c) + \Delta\bar{\mathbf{u}} \\ &= \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\lambda} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}} \qquad (5.19)\end{aligned}$$

$$\bar{\mathbf{u}}_c = 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot} + \boldsymbol{\beta} = 2\boldsymbol{\alpha}\bar{\mathbf{I}}^{\mathcal{G}} + \boldsymbol{\beta} = \bar{\boldsymbol{\lambda}} \tag{5.20}$$

The above controller equations displays how the actuators of the secondary controller, $\mathbf{u}_{tot}$, are being affected by the attack and validates that cyber controller input, $\mathbf{u}_c$, is undisturbed. The cyber controller input is then identical to the one of the unforced system and, consequently, the equal incremental costs criteria is ensured at the new equilibrium point of the controller.

Equation 5.19 shows that the secondary controller is perturbed by the attack and it is necessary to asses how the maligned values affects the physical network. It is previously shown in *Part A* Section 3.1.2 how the

secondary controller is modelled as the voltage controller in the DGs. It is therefore necessary to assess if the perturbed secondary controller still is qualified to ensure average voltage regulations at the new equilibrium point. This is done by implementing the secondary controller into the average voltage regulation of the physical network as presented below. The voltage control is previously defined in *Part A* in equation 1.1.2 and is, at the the equilibrium defined as: $\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \bar{\mathbf{u}}_{tot}$.

$$\begin{aligned}\bar{\mathbf{V}} &= \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \bar{\mathbf{u}}_{tot} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\lambda} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}} \\ &= \mathbf{1}V_{nom} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\lambda} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}} \end{aligned} \tag{5.21}$$

The individual weightings of the pre-defined interconnection patters are then added to the voltage control as below. The goal is to guarantee functioning weighted average voltage regulation at the equilibrium point, defined when: $\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom}$.

$$\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top\mathbf{w}\left[2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\lambda} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}}\right] \tag{5.22}$$

Recall that the weightings are defined equal to $\frac{1}{2\boldsymbol{\alpha}}$, and the final weighted average voltage regulation of the forced system is expressed as:

$$\begin{aligned}\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top\mathbf{w}\left[\mathbf{w}^{-1}(-K_p\mathcal{L}\bar{\lambda} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}}\right] \\ &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top\mathbf{w}\Delta\bar{\mathbf{u}}\end{aligned} \tag{5.23}$$

The first terms within the brackets are cancelled out due to the Laplacian property $\mathbf{1}^\top\mathcal{L} = 0$, $\mathbf{w}\mathbf{w}^{-1} = \mathbf{1}$ and due to $K_p$ being defined as a constant value. The final average voltage regulation at the new equilibrium point is therefore proven unsatisfied as term related to the cyber attack maintains and the weighted sum of the voltages is not equal to $\mathbf{V}_{nom}$. The above equation also shows that increasing the primary control parameter will only increase the influence of the attack as $\mathbf{w}^{-1} = 2\boldsymbol{\alpha}$ and the proposed resilient controller in *Hypothesis* 1 is not a sufficient controller to mitigate the effects of the cyber attack in terms of average voltage regulation.

## 5.6 Simulations of the Attacked System

The previously simulated unforced cyber-physical microgrid is now simulated as a perturbed system exposed to cyber attacks in the control actuators. The CP MG is simulated in Simulink with equal inherent dynamics as in *Part A* Section 4, and the attack is simulated by adding values on top of the actual controller outputs of the cyber layer. The values of the arbitrary implemented attack vector are: $\Delta\mathbf{u} = [5, 1, 0, 10]^\top$. The attack is simulated to perturb in the time interval $[5, 20]$ seconds while the previously established inherent events still are occurring as defined in Table 4.1. The unforced system's control parameters are presented in Table 4.2 and is now assessed combined with the inherent system changes and additional false data injected into actuators. The system response when exposed to the cyber attacks is firstly assessed and then the proposed resilient controller is tested in order to see if the influence of the cyber attack is removed with high $\boldsymbol{\alpha}$.

The voltage control at the new equilibrium point is simulated by using the same approach and equation established for the voltage plot of the unforced system. This is a valid voltage control representation for the forced system as the desired response is that perturbation term below is eliminated by the resilient controller and the system converges to the same equilibrium as the unforced system. The voltage control is therefore validated if the weighted sum of the measured DG voltages are equal to $48V$ while the system is under attack.

$$\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top\mathbf{w}\Delta\mathbf{u} \tag{5.24}$$

Figure 5.4 and 5.5 shows the system response when the cyber attack is intruding the system between 5 and 20 seconds. The perturbed system is validated to not maintain the average voltage regulation when the attack is intruding and vanishing. However, Figure 5.4 shows that even with the cyber attack the cyber network manages to establish one consensus value and the proposed PI-controller is able to satisfy control objective *1*. It is also recognized that the consensus value is increased at the time steps when the attack is intruding and reduced when the attack is vanishing. Even though the first control objective is satisfied, the incremental costs are affected by the attack, not obtaining the same optimal equal incremental cost as the unforced system at the time steps 5 seconds and 20 seconds. However, the objective is to ensure the two control objectives at the equilibrium: i.e., in steady state and the transient responses at 5 and 20 seconds are disregarded and left for further work studying the transient control performance. It is observed that the steady state consensus value is so close to the consensus value of the unforced system and the control objective *1* is assumed satisfied.

Figure 5.3: Perturbed MG under CA1

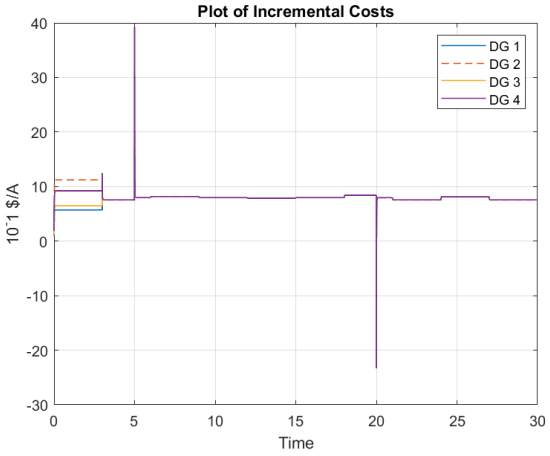


Figure 5.4: Incremental costs of perturbed system

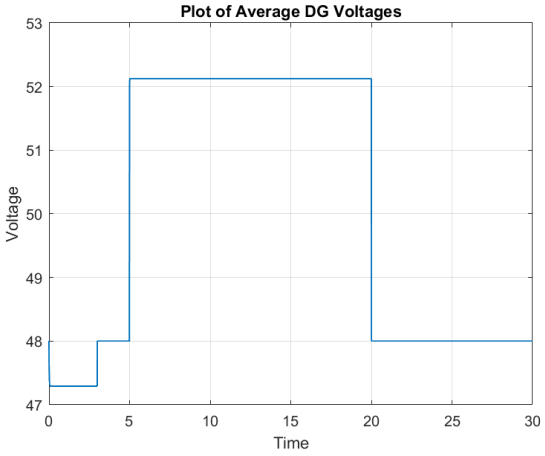


Figure 5.5: Average voltage of perturbed system

The resilient controller is now tested on the case specific MG while simulating the bounded attacks in the actuators. $\boldsymbol{\alpha}$ is tuned to 3000, defined in the *Appendix* B as the minimum parameter value necessary in order to reduce the influence of all cyber attacks when the resilient control strategy from *Hypothesis* 1 is applied.

In the above sub-sections, the mathematically derived conclusion states that the control objective *1* is ensured at the new equilibrium while the system is under attack, while not ensuring control objective *2*. The tuning of the control parameter $\boldsymbol{\alpha}$ is described to not have any affect on the voltage control or the ability to ensure consensus. This conclusion is validated and visualized in Figure 5.7 and 5.8 where the plots presents the system's incremental costs and average voltage response with $\boldsymbol{\alpha} = 3000$.

Figure 5.6: Primary Control Parameter Tuned to 3000

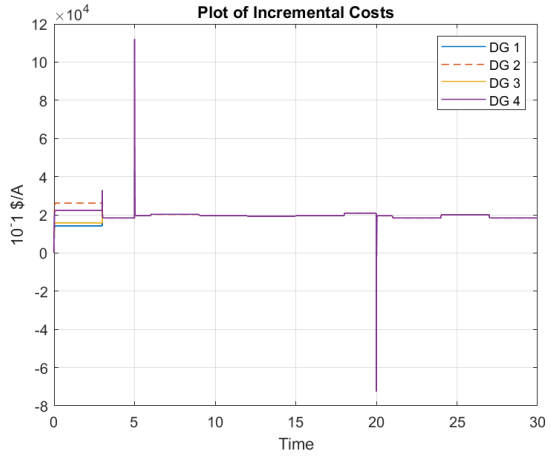


Figure 5.7: Incremental costs of perturbed system, with primary controller tuned to 3000

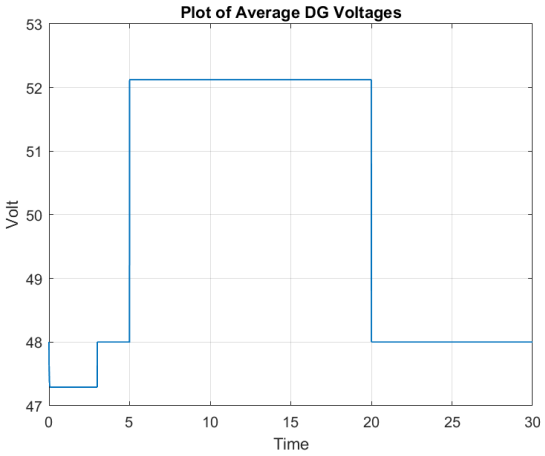


Figure 5.8: Average voltage of perturbed system, with primary controller tuned to 3000

The above figures displays that the system is unchanged with respect to the tuning of $\boldsymbol{\alpha}$ and the resilient controller needs to be modified in order to satisfy both desired objectives as the new equilibrium while the system is under attack in the actuators.

## 5.7 Conclusion of the System Analysis while Subject to Cyber Attack 1

In the above sub-sections the first potential cyber attack is added to the system dynamics: i.e., constructing the attack and fabricating the perturbed system. The stored energy, power preserving interconnections and

energy changes within the sub-networks are then assessed and it is concluded that the closed loop system is converging to a steady state equilibrium point as close as possible to the desired equilibrium due to the bounded attack. This new equilibrium is then assessed, evaluating the performance of the controller while the MG is under attack in the actuators. It is shown that the proposed control system is able to ensure the first control objective as the cyber units are cooperatively conducting one consensus value at the converged equilibrium. However, average voltage regulation is not fully ensured at the closest equilibrium within the bound defined by the attack. This will therefore again affect the actual values of the incremental costs at the times where the attack is intruding and vanishing from the system. The unsatisfied average voltage regulation leads to less optimal currents, again leading to potential false incremental cost values. However, the simulations show that the steady state consensus value is approximately equal to the steady state consensus value of the unforced system. It is therefore valid to conclude that the control objective *1* is satisfied.

In *Part B* Section 2.4 the proposed controller was assumed able to eliminate the attack by tuning the primary control parameter to a significant high value. By studying the dynamical average voltage regulation at the equilibrium it is shown that the proposed resilient controller is not able to eliminate the perturbation term as neither $\boldsymbol{\Delta u}$ nor the secondary controller $\mathbf{u}_{tot}$ is multiplied with the control parameter $\boldsymbol{\alpha}$. It is therefore concluded that the controller needs to be modified in order to ensure the two main control objectives at the new equilibrium while the system is under attack in the actuators.

# 6 Cyber Attack 2: Attacking the Current Sensors in the Physical System

The second cyber attack under consideration is a FDIA perturbing in the current measurements of the DGs. The current sensors are located in the converters of the DGs and the potential cyber attack adds false data on top of the measured currents in the generators. This is possible due to the fact that the DGs are the communicating units in the cyber layer. The maligned current values are then transferred through both the primary droop control loop and communicated to the control network as visualized in Figure 6.1. Even though the FDIA is maligning the values of the measured currents in the physical network, the attack is only perturbing the control configurations and not the existing electrical connections. The false data are therefore not transferred trough the edges of the generators and will not directly affect the consumption in the loads. When the false data are brought to the cyber layer, the secondary controller delivered to the physical layer then will have maligned values. Hence, the disturbed $\mathbf{u}_{tot}$ will then steer the generating units with a false control input, causing faulty power generation and the power delivered to the loads are of invalid values. It is therefore necessary to study how this inaccurate power control affects the energy of the closed loop MG under steady state operations and assess if false measured values affects the average voltage regulation.

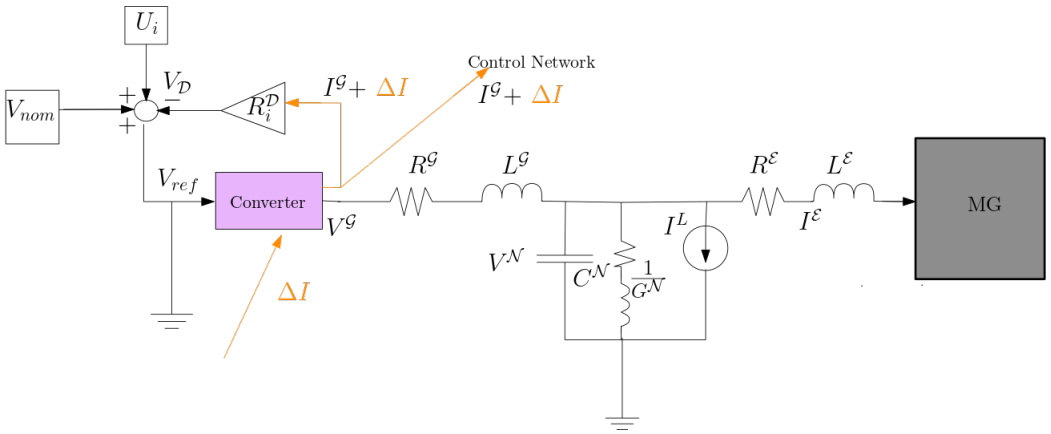


Figure 6.1: Electrical network with cyber attack in current sensor

The following analyses of the perturbed system subject to cyber attacks in the current sensors, are conducted with the same objectives and methodology as in the previously studied perturbed system subject to the first cyber attack. Each step of the system analysis below is further discussed and theoretically supported in the previous *Part B* Section 5.

## 6.1 Cyber Attack Modelling

In order to later assess the perturbed system with respect to stability and performance, the cyber attack needs to be constructed with respect to the inherent dynamics of the cyber-physical MG. The DC MG studied in this thesis admits the pH formalism and the state space model is expressed below, modified to include the potential attack, $\Delta\mathbf{I}$, in the current sensors. $\Delta\mathbf{I}$ is therefore defined as a $(4 \times 1)$ column vector in order to add false values with respect to all four DGs. The $\mathbf{A}$-matrix will include the same dynamics as the unforced system and the dynamical input matrix $\mathbf{B}$ contains the structural information concerning how the attack infiltrates the DGs. Even though the attack is infiltrating in the electrical network, the false data will only linearly enter and malign the values of the generating units through the control input; i.e., with respect to the time-derivative of the generator states $\dot{\boldsymbol{\phi}}^{\mathcal{G}}$ and the controller states $\dot{\mathbf{x}}_c$. This is represented in the below pH system representation

where the **B**-matrix only consist of dynamics with respect to the aforementioned states.

$$\begin{bmatrix} \dot{\boldsymbol{\phi}}^{\mathcal{G}} \\ \dot{\boldsymbol{\phi}}^{\mathcal{E}} \\ \dot{\mathbf{q}}^{\mathcal{N}} \\ \dot{\mathbf{x}}^{c} \end{bmatrix} = \begin{bmatrix} \left[2\boldsymbol{\alpha}(-K_p\mathcal{L}2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \left[-\mathcal{B}^{\mathcal{G}\top}\right] & \left[2\boldsymbol{\alpha}\mathcal{L}\right] \\ 0 & \left[-\mathbf{R}^{\mathcal{E}}\right] & \left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \left[\mathcal{B}^{\mathcal{G}}\right] & \left[\mathcal{B}^{\mathcal{E}}\right] & \left[-\mathbf{G}^{cte}\right] & 0 \\ \left[-\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^{c} \end{bmatrix} + \begin{bmatrix} \left[-2\boldsymbol{\alpha}K_p\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \left[-\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta\mathbf{I} \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{6.1}$$

**Closed Loop Control System**

The final control system of the unforced system is then modified to include the cyber attacks. The same interconnection pattern of the unforced system is still certified as the attack vector is implemented with the same control dynamics as the generator currents. This is recognized below where the lossy skew-symmetric matrix containing the control dissipation and the interconnection weightings, is added in front of the output vectors and equally added in front of the attack vector.

$$\begin{aligned} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} &= \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \Delta\mathbf{I} \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} & -(2\boldsymbol{\alpha}) \\ (2\boldsymbol{\alpha})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ \boldsymbol{\beta} \end{bmatrix} + \begin{bmatrix} \mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} \\ (2\boldsymbol{\alpha})^{\top} \end{bmatrix} \Delta\mathbf{I} \end{aligned} \tag{6.2}$$

With the above closed control network, and added attack vector, the dynamics of the secondary controller are expressed in scalar form below.

$$\begin{cases} u_{tot} = R_i^D(I_i^{\mathcal{G}} + \Delta I) + 2\alpha_i(K_p z_i^{\lambda} - z_i^c) \\ \qquad = R_i^D(I^{\mathcal{G}} + \Delta I) + 2\alpha(-K_p\mathcal{L}\lambda + \mathcal{L}K_i^I x_i^c) \\ \dot{x}_i^c = z_i^{\lambda} \\ z_i^{\lambda} = \sum_{j\in\mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) \\ z_i^c = \sum_{j\in\mathcal{N}_c} a_{ij}K_i^I(x_j^c - x_i^c) \\ \lambda_i = 2\alpha_i(I_i^{\mathcal{G}} + \Delta I) + \beta_i \end{cases} \tag{6.3}$$

All the dynamics of the MG are now modified to be subject to FDI attacks in the current sensors of the DGs. The perturbed CP MG can then be assessed with respect to bounded stability and its resilience is tested.

## 6.2 Energy Flow Analysis

The first part of the energy analysis is to assess the power flows of the closed loop MG while the system is under attack in the current measurements. The interconnection pattern is presented below, showing that the attack modifies the interconnections as a constant source vector. The added false data will affect both the secondary controller $\mathbf{u}_{tot}$ and the cyber controller input $\mathbf{u}_c$ in the closed loop system given in 6.2.

$$\begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} = \mathbf{F}_L \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \mathbf{F}_L\Delta\mathbf{I} = \mathbf{F}_L \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \begin{bmatrix} -\mathbf{r}\Delta\mathbf{I} \\ \mathbf{w}^{-1}\Delta\mathbf{I} \end{bmatrix} \tag{6.4}$$

In the above representation the weightings and added dissipation of the secondary controller are implemented in the lossy interconnection matrix $\mathbf{F}_L$. As the attack is perturbing in the control of electrical system the added false values are brought to the cyber layer, flowing through the cyber network and brought back to the physical network via the secondary control input. The two controllers of the closed loop control system, including the cyber attack, are defined as: $\mathbf{u}_{tot} = \mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c - \mathbf{r}\Delta\mathbf{I} + \mathbf{b}$ and $\mathbf{u}_c = \mathbf{w}^{-1\top}\mathbf{y}_{tot} + \mathbf{w}^{-1}\Delta\mathbf{I} + \mathbf{b}_c$.

### 6.2.1 Power Flows

The Hamiltonian of the interconnected MG is previously defined as unchanged regardless of potential cyber attacks as the intrinsic physical dynamics are unchanged. The Hamiltonian is therefore defined equal to the previously specified energy function: $H_T(x_T) = H_{tot}(x_{tot}) + H_c(x_c) = \frac{1}{2}\mathbf{x}_{tot}^{\top}\mathbf{Q}_{tot}\mathbf{x}_{tot} + \frac{1}{2}\mathbf{x}_c^{\top}\mathbf{K}_I\mathbf{x}_c$.

The time derivative of the stored energy in open loop is previously given as the sum of the energy changes in the two separate sub-systems. The time derivative of the Hamiltonian, while the system is under attack in the current sensors, is then expressed as:

$$\begin{aligned}\dot{H}_T(x_T) &= \dot{H}_{tot}(x_{tot}) + \dot{H}_c(x_c) \\ &= \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{F}_{tot}\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot}^{\mathcal{G}} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c \quad (6.5)\end{aligned}$$

The interconnection pattern is then used to express the control parameters as a function of the associated port variables, and thus closing the loop. The intention is to see if some terms of the time-dependent Hamiltonian are cancelling out due to power preservation.

When closing the control loop the first term of $\dot{H}_T$ describes the energy dissipation of the interconnected MG caused by the inherent dynamics of the system. The **r**-term in 6.6 is added to $\mathbf{F}_{tot}$ establishing a new dissipation matrix $\mathbf{T}_T$ adding dissipation with respect to the physical states in the electrical network. The first term of $\dot{H}_T$ is then split into power conservation and power dissipation of the closed loop system. Power conservation is a physical requirement and does not change over time, and the first term is defined equal to the power dissipation of the physical network. Term two and four are related to the energy exchanged between the cyber layer and physical layer and if the power is preserved the two terms will cancel out, as previously proven valid for the unforced system. The exchanged output from the electrical layer $\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}$ is previously defined equal to the transposed output value of the network $\mathbf{y}_{tot}^\top$. The same yields for the output $\boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c$ equal to the transposed output of the control network, $\mathbf{y}_c^\top$. When also exploiting the skew-symmetric properties given in *Part B* Section 6.2, the separate syb-system's change in energy are expressed as below by exploiting the interconnection pattern given in 6.4.

$$\begin{aligned}\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} &= \mathbf{y}_{tot}^\top\mathbf{u}_{tot} \\ &= \mathbf{y}_{tot}^\top(\mathbf{r}\mathbf{y}_{tot} - \mathbf{w}^{-1}\mathbf{y}_c - \mathbf{r}\Delta\mathbf{I} + \mathbf{b}) \\ &= -\mathbf{y}_{tot}^\top\mathbf{r}\mathbf{y}_{tot} - \mathbf{y}_{tot}^\top\mathbf{w}^{-1}\mathbf{y}_c - \mathbf{y}_{tot}^\top\mathbf{r}\Delta\mathbf{I} + \mathbf{y}_{tot}^\top\mathbf{b} \quad (6.6) \\ \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c &= \mathbf{y}_c^\top\mathbf{u}_c \\ &= \mathbf{y}_c^\top(\mathbf{w}^{-1^\top}\mathbf{y}_{tot} + \mathbf{w}^{-1}\Delta\mathbf{I} + \mathbf{b}_c) \\ &= \mathbf{y}_c^\top\mathbf{w}^{-1^\top}\mathbf{y}_{tot} + \mathbf{y}_c^\top\mathbf{w}^{-1}\Delta\mathbf{I} + \mathbf{y}_c^\top\mathbf{b}_c \quad (6.7)\end{aligned}$$

The above equations validates some power preserving properties in the interconnections between the two networks as: $-\mathbf{y}_{tot}^\top\mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_c^\top\mathbf{w}^{-1^\top}\mathbf{y}_{tot} = 0$, due to transformed matrix properties. The final time-dependent energy function is given below depending on both induced/reduced electrical energy and cyber energy in regards to the attack.

$$\begin{aligned}\dot{H}_T(x_T) &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) - \mathbf{y}_{tot}^\top(-\mathbf{r}\Delta\mathbf{I} + \mathbf{b}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \mathbf{y}_c^\top\mathbf{w}^{-1}\Delta\mathbf{I} \\ &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}(\mathbf{r}\Delta\mathbf{I} + \mathbf{b}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} \quad (6.8) \\ &\qquad + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c(\mathbf{w}^{-1}\Delta\mathbf{I} + \mathbf{b}_c)\end{aligned}$$

## 6.3 Stability Analysis

The next step in the analysis of the perturbed system, is to assess the stability by means of the Lyapunov stability criteria. The analysis assesses if the system is converging to steady state at an equilibrium, preferably the desired one, while being under attack in the current sensors. The stability analysis is based on *Lemma 4.5* defined in [23], equal to the lemma used in the stability analysis of system prone to cyber attacks in the actuators of the controller. *Input - to - state stability* is therefore actually already proven for the perturbed CP MG of study, as the analysis is conducted by ignoring the bounded attack and assessing if the unforced system is proven exponentially stable. All the studied perturbed systems prone to the different cyber attacks, are based on the same unforced CP MG and the studied systems in this thesis are proven ISS regardless of the cyber attacks. The deduction of the Lyapunov stability assessment is therefore only explained in details in *Part B* Section 5.3.2. However, from a didactic point of view it is still useful to show that the final Lyapunov candidate, with added cyber attack 2, is expressed as the dissipation of the closed loop MG and added/reduced energy source introduced by the bounded attacks. When the *bounded - input - bounded state* property is defined in the final Lyapunov function, the ISS is concluded for the perturbed system. The first step in order to obtain the Lyapunov is to bring the energy functions to the incremental level.

### 6.3.1 Incremental Energy Modelling

The incremental states of the closed loop system are defined equally as in 5.10 where $\tilde{\mathbf{x}} = \mathbf{x} - \bar{\mathbf{x}}$. Briefly explained, the incremental energy modelling is necessary in order to study the stability of the system at the steady state equilibrium point. The Lyapunov function is based on incremental energy, it requires the energy function to have a minimum at the point of interest. Hence, the energy changes of the closed loop MG is then defined below with incremental energy. All constants are being cancelled out and the attacks are implemented as time varying inputs – also expressed with incremental energy.

$$\dot{H}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{r}\Delta\tilde{\mathbf{I}} + \boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\mathbf{w}^{-1}\Delta\tilde{\mathbf{I}} \tag{6.9}$$

### 6.3.2 Lyapunov Stability Criteria

The incremental energy functions of the perturbed system subject is then defined below. The functions are influenced by the energy function specified as $H(\tilde{x}_T)$, and the time-dependent energy function $\dot{H}(\tilde{x}_T)$.

$$\begin{aligned} V_T(\tilde{x}_T) &= H_{tot}(\tilde{x}_{tot}) + H_c(\tilde{x}_c) \\ &= \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top\mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top\mathbf{K}_I^{-1}\tilde{\mathbf{x}}_c \end{aligned} \tag{6.10}$$

$$\dot{V}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{r}\Delta\tilde{\mathbf{I}} + \boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\mathbf{w}^{-1}\Delta\tilde{\mathbf{I}} \tag{6.11}$$

The stability of the system and the ability to ensure steady state operations at the equilibrium is then proven satisfied as the Lyapunov function above holds the BIBS property. The system is proven to exponentially converge to the steady state equilibrium within the bound of the attack: i.e., the steady state equilibrium closest to the desired equilibrium.

## 6.4 Equilibrium Analysis

The above analysis confirms that the *Assumption* 1 remains valid when the system is subject to cyber attack in the current sensors i.e the closed loop MG converges to a new equilibrium and the two sub-systems have individual equilibriums. The Lyapunov function is bounded by the attack vector and the system operates under ISS conditions. The next step in the system analysis is therefore to assess if the proposed resilient control strategy given in *Hypothesis* 1 is able to ensure the two defined control objectives, equal incremental costs and average voltage regulation, at this new equilibrium point.

The primary control objective is to guarantee that the DGs are able to agree on one consensus value for the incremental costs of generation in steady state. The equilibrium point of the distributed control network is therefore firstly assessed as $\lambda_i$ are the communicated values of closed loop. The desired result of the consecutive analysis is that the cyber states are brought to steady state operations due to the Laplacian property combined with the cooperatively obtained optimal value of the incremental costs. The dynamics of the controller states of the forced system is defined in *Part B* Section 6.3 as $\dot{\mathbf{x}}_c = \mathbf{z}^\lambda = -\mathcal{L}\boldsymbol{\lambda} = -\mathcal{L}((2\boldsymbol{\alpha}\mathbf{I} + \Delta\mathbf{I}) + \boldsymbol{\beta})$. The steady state of the control network is then expressed below.

$$\sum_c^- : \begin{cases} 0 = \mathbf{g}_c\bar{\mathbf{u}}_c \\ \bar{\mathbf{y}}_c = \mathbf{g}_c^\top\boldsymbol{\nabla}H_c(\bar{\mathbf{x}}_c) \end{cases} \longrightarrow \begin{cases} 0 = -\mathcal{L}(2\boldsymbol{\alpha}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta}) \\ \bar{\mathbf{y}}_c = -\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \end{cases} \longrightarrow \begin{cases} 0 = -\mathcal{L}\bar{\boldsymbol{\lambda}}^* \\ \bar{\mathbf{y}}_c = -\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \end{cases} \tag{6.12}$$

The above system representation shows that the forced control network converges to the steady state equilibrium when $-\mathcal{L}\bar{\boldsymbol{\lambda}}^*$ equals zero only evolving when $\bar{\boldsymbol{\lambda}}^* = \mathbf{1}\lambda^*$ and by using the Laplacian property. $\boldsymbol{\lambda}^*$ is then the consensus value for all the generators defined by the actual measured currents and additional attack values implemented in each current sensor. However, it is not valid to define this value equal to the optimal equal incremental cost value: i.e., $\mathbf{1}\bar{\lambda}^* \neq \mathbf{1}\bar{\lambda}_{opt}$. Even though the equilibrium analysis confirms that the controller reaches consensus at a new equilibrium point of the perturbed system, the consensus value will be of false high value compared to the unforced system's consensus value. The obtained consensus value is significantly diverging from the unforced consensus value and the control objective *1* is therefore concluded not satisfied at the new equilibrium.

The next step is to assess how the attack perturbs the closes loop control system and how the potentially perturbed secondary controller disturbs the operations of the physical network. The control system of the

forced CP MG – exposed to cyber attacks in the current sensors – are expressed above in sub-section 6.2 and are specified at the new converged equilibrium point below.

$$\begin{aligned}\bar{\mathbf{u}}_{tot} &= \mathbf{R}^D\bar{\mathbf{y}}_{tot}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} + 2\boldsymbol{\alpha}\bar{\mathbf{y}}_c \\ &= \mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}(2\boldsymbol{\alpha}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta}) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \\ &= \mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \qquad (6.13) \\ \bar{\mathbf{u}}_c &= 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta} = 2\boldsymbol{\alpha}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}})\boldsymbol{\beta} = \bar{\boldsymbol{\lambda}}^* \qquad (6.14)\end{aligned}$$

The cyber controller given in 6.14 validates that the attained consensus value will be of higher value than the optimal value of the unforced system as $\bar{\boldsymbol{\lambda}}^* \neq \bar{\boldsymbol{\lambda}} = \mathbf{1}\lambda_{opt}$. The cyber layer given in 6.12 presents that the cyber controller is a communicated value between the units. $\mathbf{g}_c = -\mathcal{L}$ and all properties following the Laplacian-matrix are defined as communication properties. The false data added in the current sensors are consequently communicated between the generating units, creating a higher consensus value than for the unforced system. The desired effect of the resilient controller is therefore to reduce the cooperatively defined consensus value while the system is under attack. As the primary control parameter $\boldsymbol{\alpha}$ is appearing in front of both $\mathbf{I}^{\mathcal{G}}$ and $\Delta\mathbf{I}$ the tuning of the parameter will not reduce the influence of the attack. It is therefore concluded that the proposed resilient strategy presented in *Hypothesis* 1 only boost the cooperative consensus value, including boosting the false added attack value.

The secondary controller $\mathbf{u}_{tot}$ is also displayed perturbed by the cyber attack, $\Delta\mathbf{I}$, in 6.13. Subsequently, the average voltage control objective needs to be assessed at the equilibrium of the physical network. The perturbed current sensors are firstly adding false value to the primary droop controller and subsequently the perturbed secondary controller is adding false value to the voltage control dynamics of the electrical system. The final voltage controller of the forced system, including the perturbation term, is presented below.

$$\begin{aligned}\bar{\mathbf{V}} &= \mathbf{1}V_{nom} - \mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \bar{\mathbf{u}}_{tot} = \mathbf{1}V_{nom} - \mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \\ &= \mathbf{1}V_{nom} - K_P 2\boldsymbol{\alpha}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \qquad (6.15)\end{aligned}$$

The individual weightings are then added to the voltage controller in order to assess if the electrical network achieves average voltage regulation, previously defined as: $\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom}$. The weighted voltage regulation, with the implemented perturbation terms, is specified at the physical network's equilibrium point as:

$$\begin{aligned}\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\left[K_P 2\boldsymbol{\alpha}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c\right] \\ &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} \qquad (6.16)\end{aligned}$$

The last equality is derived by using the definition $\mathbf{w} = \frac{1}{2\boldsymbol{\alpha}}$ and the Laplacian property $\mathbf{1}^\top\mathcal{L} = 0$. The perturbed primary droop control is firstly cancelled out by the perturbed secondary controller and the rest of $\mathbf{u}_{tot}$ is equal to zero due to the Laplacian. The average voltage control objective still stabilizes at the desired equilibrium point even when the system is subject to cyber attacks in the current sensor. In addition, the above equation shows that the tuning of $2\boldsymbol{\alpha} = \mathbf{w}^{-1}$ will only scale the voltages and not disturb the ability to achieve weighted average voltage equal to the pre-defined $V_{nom}$. It is therefore concluded that the tuning of the primary controller will not change the voltage response or the cost of generation at the new equilibrium.

## 6.5 Simulations of the Attacked System

The cyber-physical microgrid subject to cyber attacks in the current sensors is now simulated with arbitrary implemented attack vector $\Delta\mathbf{I} = [1, 3, 6, 0]^\top$ intruding in the time interval $[5, 20]$ seconds. The events simulated for the unforced system is still implemented in order to see the system response for regular system changes in addition to the cyber attacks. The untuned control parameters of the distributed controller are presented in Table 4.2.

The perturbed system is firstly simulated without the resilient controller strategy: i.e., the system simulations showcases the system response of the proposed case specific MG with the attacks perturbing the current sensors. The controller is untuned and the secondary controller is equally defined as for the unforced system. Figure 6.3 presents that the DGs cooperatively define one consensus value when the secondary controller is activated. However, when the attack is intruding in the time interval $[5, 20]$, the consensus value is of incorrect high value, and is therefore not defined equal to the optimal consensus value. It is not possible to plot the real incremental costs and thereby present that the costs are not equally defined for all the DGs, as there are now

way of knowing which parts of the currents that are of real or false values. However, the Figure 6.3 presents that the consensus value is so far off from the unforced system, presented in Figure 4.4, and it is therefore concluded that the control objective *1* is not satisfied.

Figure 6.4 shows that the controller is able to steer the voltages so that the sum equals to the predefined voltage: $V_{nom} = 48V$.

Figure 6.2: Perturbed MG under CA2

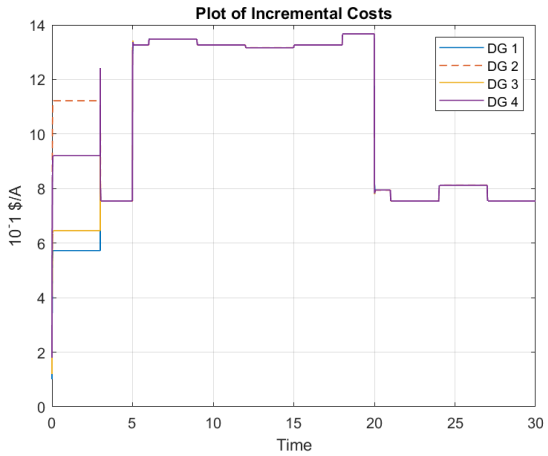


Figure 6.3: Incremental costs of perturbed system

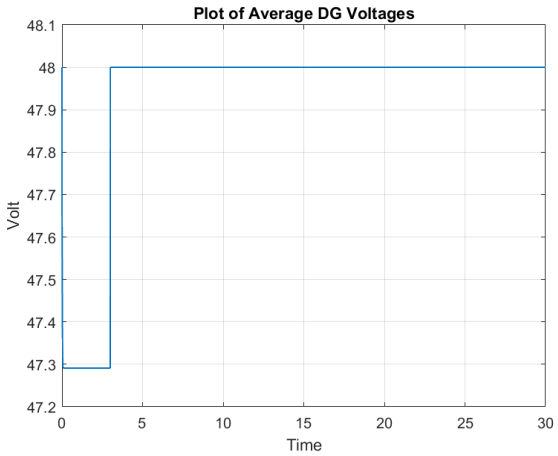


Figure 6.4: Average voltage of perturbed system

The above mathematical analyses concluded that the controller is able to achieve consensus however not satisfying the control objective *1* regardless of the proposed resilient control strategy. Equally, it was concluded that the control objective *2* were satisfied at the new equilibrium regardless of the attack in the current sensors and regardless of the tuning of $\boldsymbol{\alpha}$. Figure 6.6 and 6.7 displays the system response of the MG with the primary controller tuned to the defined resilient minimum value of 3000, defined in *Appendix* B. The system responses are featured equal as for the perturbed system with the regular PI-controller: i.e., equal system responses before and after the tuning of $\boldsymbol{\alpha}$. The simulations validates the conclusion of the resilient strategy: i.e., the tuning of the primary control parameter do not change the ability to achieve average voltage regulation or consensus. However, the tuning do not contribute in removing the influence of the attack to the point where the consensus value corresponds to the optimal equal incremental cost value.

Figure 6.5: Primary Control Parameter Tuned to 3000

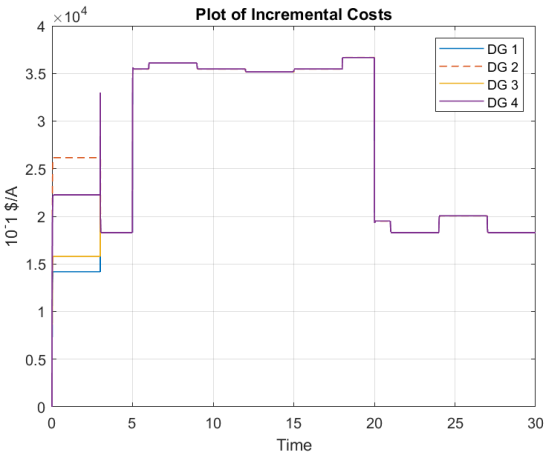


Figure 6.6: Incremental costs of perturbed system, with primary controller tuned to 3000

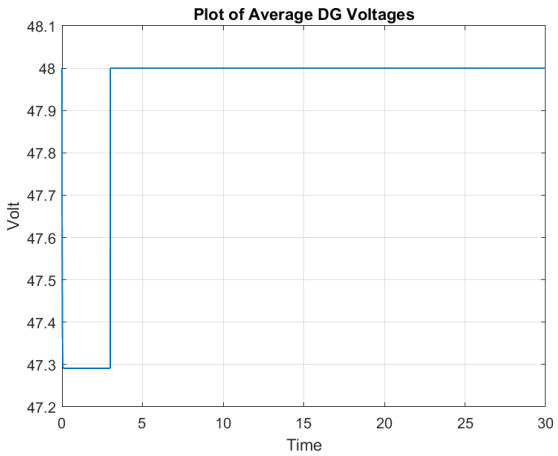


Figure 6.7: Average voltage of perturbed system, with primary controller tuned to 3000

## 6.6 Conclusion of the System Analysis while Subject to Cyber Attack 2

The above sections proves that the perturbed system converges to a new steady state equilibrium while being under attack in the current sensors. The performance of the controller is then assessed and it is shown that the closed loop control system is able to ensure average voltage regulations and cooperatively defining a consensus value. However, the consensus value is incorrect when the attack is perturbing and the controller is not able to operate the system as unforced. This is concluded both mathematically and validated with proper simulations. The effect of the high incremental costs is assumed to affect the generated power of the units, however its precise effects are considered out of scope of this investigation. When studying the control system at the equilibrium it is shown that the proposed resilient controller in *Hypothesis* 1, bringing the primary control parameter $\boldsymbol{\alpha}$ to significant high values, will not reduce the influence of the attacks. However, as the control objective *2* is satisfied it is relevant to recognize that the high primary control parameter will not reduce the ability to ensure average voltage regulation. It is then concluded that the tuning of the $\boldsymbol{\alpha}$ does not affect the objectives of the MG: it will not improve the control performance and will not damage the control performance. If the proposed resilient controller is performing as desired for other cyber attacks, then the resilient strategy may be applied when the attack intrudes the current sensors without perturbing the equilibrium and thus the control performance aiming to optimally operate the MG.

An additional conclusion drawn from the analysis above is that the FDIA actually is implemented as a *stealth attack*. The stealth attacks are often perturbing in the voltage sensors regarding the *voltage control*. However, the primary droop control of the system is equipped with current sensors in order to limit the voltage deviation. Disturbing the current sensor is therefore equivalent to disturbing the voltage control. Stealth attacks are perturbing more discretely often still ensuring the objectives of the MG and the attack is therefore more difficult to detect. As the controller ensures voltage regulation and consensus – though not the optimal consensus value – the FDIA is classified as a stealth attack. The final conclusion is then, that the controller needs to be modified to ensure that the system operates as uncompromised: i.e., modifying the controller so that the perturbation term is eliminated in the dynamical equations ensuring that the obtained consensus value corresponds to the optimal consensus value of the incremental costs.

# 7 Cyber Attack 3: Attacking the Communication Links within the Control Network

The third and final cyber attack under consideration is the third party man-in-the-middle (MITM) attack infiltration in the communication links of the distributed control network. According to the presented literature review in *Part B* Section 1, a MITM attack may interfere with the system as either a hijacking attack: i.e., completely replace the existing signals, or a false data injection attack: i.e., adding values on top of existing signals. Regardless of the behaviour of the attack, the MITM-attack changes the communicated values between the DGs in the cyber layer of the MG. The communicated values are previously defined as all the parameters following the Laplacian due to the definition where the Laplacian contains the consensus properties. In the final control system presented in *Part B* Section 3 for the unforced system, the Laplacian is appearing twice. Hence, there are two potential cyber attacks that may infiltrate the communication links as visualized in Figure 7.1. The MITM cyber attack may change/add values with respect to either the communicated incremental costs or the communicated cyber states where the associated attack vectors are respectively expressed as $\Delta\lambda$ and $\Delta x_c$.

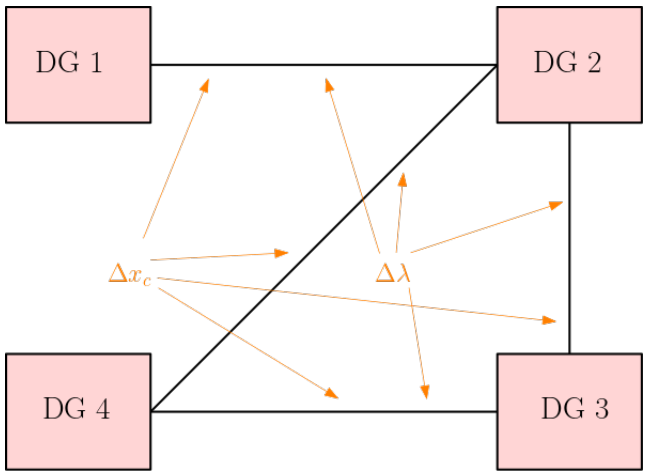


Figure 7.1: Distributed control network with cyber attacks in the communication links

As the third cyber attack perturbs the distributed control network it is assumed that the attack will disturb the controller's ability to achieve consensus. However, as the attack only intrudes in the cyber layer it is engaging to assess how this intuitions affect the secondary controller and thereby affects the operations of the physical network.

## 7.1 Cyber Attack Modelling

In order to later assess the perturbed system with respect to stability and control performance, the cyber attacks needs to be constructed with respect to the inherent dynamics of the cyber-physical MG. The MG studied in this thesis admits the pH formalism and the state space model is expressed below, modified to include the potential attacks, $\Delta\boldsymbol{\lambda}$ and $\Delta\mathbf{x}_c$ in the cyber layer. Both the attack vectors are implemented as column vector $\in \mathbf{R}^4$ in order to malign the communicated values between all the four generating units implemented in the cyber layer. The $\mathbf{A}$-matrix will include the same dynamics as the unforced system and the external input matrices $\mathbf{B}_1$ and $\mathbf{B}_2$ contains the attack infiltration dynamics necessary in order to infiltrate the power system at the desired locations. The specified attack vectors are then implemented in the final port Hamiltonian system representation given in compact form in 7.1. The additional matrices contains the dynamics depending

on the bounded attacks and therefore containing the dynamics with respect to the Laplacians.

$$\begin{bmatrix} \dot{\boldsymbol{\phi}}^{\mathcal{G}} \\ \dot{\boldsymbol{\phi}}^{\mathcal{E}} \\ \dot{\mathbf{q}}^{\mathcal{N}} \\ \dot{\mathbf{x}}^{c} \end{bmatrix} = \begin{bmatrix} \left[2\boldsymbol{\alpha}(-K_p\mathcal{L}2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \left[-\mathcal{B}^{\mathcal{G}\top}\right] & \left[2\boldsymbol{\alpha}\mathcal{L}\right] \\ 0 & \left[-\mathbf{R}^{\mathcal{E}}\right] & \left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \left[\mathcal{B}^{\mathcal{G}}\right] & \left[\mathcal{B}^{\mathcal{E}}\right] & \left[-\mathbf{G}^{cte}\right] & 0 \\ \left[-\mathcal{L}2\boldsymbol{\alpha}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^{c} \end{bmatrix} + \begin{bmatrix} \left[-2\boldsymbol{\alpha}K_p\mathcal{L}\right] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \left[-\mathcal{L}\right] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{\lambda} \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} \left[2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\right] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta\mathbf{x}_c \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{7.1}$$

**Closed Loop Control System**
The final control system is then modified to include the cyber attacks. The same interconnection pattern between the distributed control network and the physical network is still the same, yet the false values are added as an unwanted external source, entering linearly with associated dynamics. The closed loop control system of the cyber-physical attacked MG is expressed below.

$$\begin{aligned} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} &= \begin{bmatrix} -\mathbf{r} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} + \begin{bmatrix} \mathbf{r}_1 \\ 1 \end{bmatrix} \Delta\boldsymbol{\lambda} + \begin{bmatrix} \mathbf{r}_2 \\ 0 \end{bmatrix} \Delta\mathbf{x}_c \\ &= \begin{bmatrix} \mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} & -(2\boldsymbol{\alpha}) \\ (2\boldsymbol{\alpha})^{\top} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ \boldsymbol{\beta} \end{bmatrix} + \begin{bmatrix} -2\boldsymbol{\alpha}K_p\mathcal{L} \\ 1 \end{bmatrix} \Delta\boldsymbol{\lambda} + \begin{bmatrix} 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I \\ 0 \end{bmatrix} \Delta\mathbf{x}_c \end{aligned} \tag{7.2}$$

For these attacks, both the cyber controller $\mathbf{u}_c$ and the secondary controller $\mathbf{u}_{tot}$ will be maligned by the attack. $\mathbf{u}_c$ is one of the directly communicated values defined in 3.2 where $\dot{\mathbf{x}}_c = \mathbf{g}_c\mathbf{u}_c = -\mathcal{L}\mathbf{u}_c$ and the attack will therefore directly change the cyber controller. The secondary controller is defined to include the cyber states $\mathbf{x}_c$, now shown to include one of the potential attacks and the secondary controller is therefore also perturbed. The secondary controller will, in addition, be affected by the communicated incremental values shown in the unforced secondary control definition: $\mathbf{u}_{tot} = \mathbf{R}^D\mathbf{I}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\lambda + \mathcal{L}\mathbf{x}_c)$ where both the controller states and incremental costs appear behind the Laplacian.

With the above closed loop control system, and added attack vectors, the dynamics of the secondary controller is expressed in scalar form below. The defined matrices $\mathbf{z}^{*\lambda}$ and $\mathbf{z}^{*c}$ contains the attacked values, defined as $\mathbf{z}^{*\lambda} = -\mathcal{L}(\boldsymbol{\lambda} + \Delta\boldsymbol{\lambda})$ and $\mathbf{z}^{*c} = -\mathcal{L}(\mathbf{x}_c + \Delta\mathbf{x}_c)$.

$$\begin{cases} u_{tot} = R_i^D I_i^{\mathcal{G}} + 2\alpha_i(K_p z_i^{*\lambda} - z_i^{*c}) \\ \qquad = R_i^D I_i^{\mathcal{G}} + 2\alpha_i(-K_p\mathcal{L}(\lambda_i + \Delta\lambda_j) + \mathcal{L}K_i^I(x_i^c + \Delta x_j^c)) \\ \dot{x}_i^c = z_i^{\lambda} \\ z_i^{*\lambda} = \sum_{j\in\mathcal{N}_c} a_{ij}((\lambda_j + \Delta\lambda_j) - \lambda_i) \\ \qquad = \sum_{j\in\mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) + \sum_{j\in\mathcal{N}_c} a_{ij}\Delta\lambda_j \\ z_i^{*c} = \sum_{j\in\mathcal{N}_c} a_{ij}K_i^I((x_j^c + \Delta x_j^c) - x_i^c) \\ \qquad = \sum_{j\in\mathcal{N}_c} a_{ij}K_i^I(x_j^c - x_i^c) + \sum_{j\in\mathcal{N}_c} a_{ij}K_i^I\Delta x_j^c \end{cases} \tag{7.3}$$

## 7.2 Energy Flow Analysis

The first part of the energy analysis include assessing the power flow of the closed loop MG while the system is under attack in the communication links. The interconnection pattern with the potential attacks are presented above in 7.2, showing that the power preserving interconnections are affected by an undesired source vector due to the attacks. The two controllers are in closed loop defined as: $\mathbf{u}_{tot} = -\mathbf{r}\mathbf{y}_{tot} + \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{b} + \mathbf{r}_1\Delta\boldsymbol{\lambda} + \mathbf{r}_2\Delta\mathbf{x}_c$ and $\mathbf{u}_c = 2\boldsymbol{\alpha}\mathbf{y}_{tot} + \mathbf{b}_c + \Delta\boldsymbol{\lambda}$. $\mathbf{r}_1$ is defined equal to $-\mathbf{w}^{-1}K_p\mathcal{L}$ and $\mathbf{r}_2$ equal to $-2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I$.

### 7.2.1 Power Flows

The Hamiltonian of the closed loop MG is previously defined as unchanged regardless added attacks due to the fact that the cyber attacks cannot change the inherent physical dynamics. The Hamiltonian will therefore be equal to the previously specified energy function of the unforced system: $H_T(x_T) = H_{tot}(x_{tot}) + H_c(x_c) = \frac{1}{2}\mathbf{x}_{tot}^{\top}\mathbf{Q}_{tot}\mathbf{x}_{tot} + \frac{1}{2}\mathbf{x}_c^{\top}\mathbf{K}_I\mathbf{x}_c$.

The time derivative of the stored energy of the open loop system is, as previously defined, given as the sum of the energy changes in the two separate sub-systems–without taking into account the interconnection pattern. The time derivative of the Hamiltonian, is then defined as:

$$\begin{aligned}\dot{H}_T(x_T) &= \dot{H}_{tot}(x_{tot}) + \dot{H}_c(x_c) \\ &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{R}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot}^{\mathcal{G}} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c\end{aligned} \tag{7.4}$$

The power flow of the interconnected MG is then assessed by closing the control loop and evaluating how the energy is changing within the interconnected network. The final time-dependent energy function of the closed loop MG is then expressed by the terms contributing with added and/or reduced energy due to the attack and inherent dissipation. This function is then later used to analyse the stability, as a power system with constantly increasing energy will become unstable.

As previously presented in *Part A* 1.13, the pH model of the electrical network expresses the exchanged output $\mathbf{y}_{tot}$ equal to $\mathbf{g}_i^{\mathcal{G}\top}\boldsymbol{\nabla}H_{tot}(x_{tot})$. Equally the passive output of control network $\mathbf{y}_c$ is in *Part A* 2.10 defined as $\mathbf{g}_c^\top\boldsymbol{\nabla}H_c(x_c)$. When also exploiting the lossy skew-symmetric properties of the closed loop MG, the separate sub-systems energy changes are expressed as:

$$\begin{aligned}\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\mathbf{u}_{tot} &= \mathbf{y}_{tot}^\top\mathbf{u}_{tot} \\ &= \mathbf{y}_{tot}^\top(-\mathbf{r}\mathbf{y}_{tot} + \mathbf{w}^{-1}\mathbf{y}_c + \mathbf{b} + \mathbf{r}_1\Delta\boldsymbol{\lambda} + \mathbf{r}_2\Delta\mathbf{x}_c) \\ &= \mathbf{y}_{tot}^\top\mathbf{r}\mathbf{y}_{tot} - \mathbf{y}_{tot}^\top\mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_{tot}^\top\mathbf{b} + \mathbf{y}_{tot}^\top\mathbf{r}_1\Delta\boldsymbol{\lambda} + \mathbf{y}_{tot}^\top\mathbf{r}_2\mathbf{x}_c \qquad (7.5) \\ \boldsymbol{\nabla}^\top H_c(\boldsymbol{x}_c)\mathbf{g}_c\mathbf{u}_c &= \mathbf{y}_c^\top\mathbf{u}_c \\ &= \mathbf{y}_c^\top\mathbf{w}^{-1}\mathbf{y}_{tot} + \mathbf{y}_c^\top\mathbf{b}_c + \mathbf{y}_c^\top\Delta\boldsymbol{\lambda} \qquad (7.6)\end{aligned}$$

The final time derivative of the Hamiltonian is then defined below for the closed loop. The first term is equal for all the cyber attacks as it is only expressed with respect to the physical dynamics implemented for the unforced system. Hence, the first term is previously proven equal to power dissipation due to the $\mathbf{T}_T$-matrix containing the electrical dissipation and the PI-control dissipation $\mathbf{r}$.

$$\begin{aligned}\dot{H}_T(x_T) &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) + \mathbf{y}_{tot}^\top\mathbf{b} + \mathbf{y}_{tot}^\top\mathbf{r}_1\Delta\boldsymbol{\lambda} + \mathbf{y}_{tot}^\top\mathbf{r}_2\mathbf{x}_c + \mathbf{y}_c^\top\mathbf{b}_c + \mathbf{y}_c^\top\Delta\boldsymbol{\lambda} \\ &= -\boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}(\mathbf{b} + \mathbf{r}_1\Delta\boldsymbol{\lambda} + \mathbf{r}_2\Delta\mathbf{x}_c) + \boldsymbol{\nabla}^\top H_c(\boldsymbol{x}_c)\mathbf{g}_c(\mathbf{b}_c + \Delta\boldsymbol{\lambda})\end{aligned} \tag{7.7}$$

The above $\dot{H}_T$ function shows that two terms will cancel out due to power preservation. These are given as:$\mathbf{y}_{tot}^\top\mathbf{w}^{-1}\mathbf{y}_c + \mathbf{y}_c^\top\mathbf{w}^{-1\top}\mathbf{y}_{tot} = 0$. The final $\dot{H}_T(x_T)$ characterizes bounded energy due to the bounded attacks which again affect the stability as presented in the section below.

## 7.3 Stability Analysis

When the stability of the second perturbed system where assessed it was declared that the system was already proven ISS stable in *Part B* Section 5.3.2. This is due to the fact that the unforced systems are identical regardless of the potential attacks and *Lemma 4.5* defined in [23] describes that if the unforced system is proven to achieve exponential stability then the perturbed system is defined ISS. However, defining the Lyapunov function of the system and validate the BIBS property is a good visualisation substantiating the system's ability to achieve ISS stability bounded by the external cyber attacks. Additionally, the final Lyapunov function may later be used to calculate the actual value of the bound and potentially decrease the bound ensuring the the system converges to an even closer equilibrium in regards to the desired equilibrium.

### 7.3.1 Incremental Energy Modeling

The incremental states of the closed loop system is previously defined in 5.10 expressed as: $\dot{\tilde{x}}_T = (\mathbf{J}_{tot} - \mathbf{T}_T)\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) + \mathbf{g}_i^{\mathcal{G}}\tilde{\mathbf{u}}_{tot} + \mathbf{g}_c\tilde{\mathbf{u}}_c$. When the Lyapunov function is proposed in the next section, it is influenced by the Hamiltonian of the closed loop MG based on the incremental states. All constants are being cancelled out and as the attacks are implemented as continuous time varying inputs they are also expressed with incremental energy: $\Delta\tilde{\boldsymbol{\lambda}}$ and $\Delta\tilde{\mathbf{x}}_c$.

### 7.3.2 Lyapunov Stability Criteria

The Lyapunov function of the MG prone to cyber attacks in communication links is derived with the same approach as for the two already studied attacks. The proposed storage function $\dot{V}_T(\tilde{x}_T)$ is influenced by the time-dependent energy functions defined in 7.7. The Lyapunov candidate and associated time-dependent energy function, with the added attacks, are specified below.

$$V_T(\tilde{x}_T) = H_{tot}(\tilde{x}_{tot}) + H_c(\tilde{x}_c) = \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top \mathbf{K}_I^{-1}\tilde{\mathbf{x}}_c \tag{7.8}$$

$$\begin{aligned}\dot{V}_T(\tilde{x}_T) = &-\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\left(\mathbf{r}_1\Delta\tilde{\boldsymbol{\lambda}} + \mathbf{r}_2\Delta\tilde{\mathbf{x}}_c\right) \\ &+ \boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\Delta\tilde{\boldsymbol{\lambda}}\end{aligned} \tag{7.9}$$

The stability of the system and the ability to ensure optimal operations at the equilibrium point is then proven valid as the Lyapunov function is defined by the BIBS property. In addition to the electrical dissipation, all the increased/reduced energy is bounded by the added values from the bounded attacks. The system is proven to exponentially converge to the steady state equilibrium point within the bound of the attack: i.e., the steady state equilibrium closest to the desired equilibrium.

## 7.4 Equilibrium Analysis

The above analysis confirms that the *Assumption* 1 remains valid when the system is subject to the studied cyber attack i.e the closed loop MG converges to a new equilibrium and the two sub-systems have individual existing equilibriums. The Lyapunov function is bounded by the attack vectors and the system operates under ISS conditions. The next step in the system analysis is therefore to assess if the proposed distributed controller is able to ensure the two defined control objectives, equal incremental costs and average voltage regulation, at the new equilibrium point.

With the potential cyber attacks in the communication links, it is previously assumed that the system is not able to achieve consensus and the equal incremental cost objective is not satisfied at the new equilibrium. The distributed control network presented in 3.2 in *Part B*, defined that the states of the controller, $\mathbf{x}_c$, are a function of the Laplacian matrix multiplying the cyber controller, $\mathbf{u}_c$. The cyber controller is previously defined as the incremental costs of generation, and as it appears after the Laplacian, the incremental costs are one of the communicated values and thereby prone to MITM attacks. When closing the loop in 7.2 the secondary controller is expressed as $\mathbf{u}_c = (2\boldsymbol{\alpha}\mathbf{y}_{tot} + \boldsymbol{\beta}) + \Delta\boldsymbol{\lambda} = \boldsymbol{\lambda} + \Delta\boldsymbol{\lambda}$. The controller states of the perturbed system are then defined as:

$$\dot{\mathbf{x}}_c = -\mathcal{L}\mathbf{u}_c = -\mathcal{L}\left((2\boldsymbol{\alpha}\mathbf{y}_{tot} + \boldsymbol{\beta}) + \Delta\boldsymbol{\lambda}\right) = -\mathcal{L}(\boldsymbol{\lambda} + \Delta\boldsymbol{\lambda}) \tag{7.10}$$

In order to ensure consensus and equal incremental costs at the equilibrium point, the controller is evaluated at point where time derivative of the system is zero i.e at steady state.

$$0 = \mathbf{g}_c\bar{\mathbf{u}}_c = -\mathcal{L}\left((2\boldsymbol{\alpha}\mathbf{y}_{tot} + \boldsymbol{\beta}) + \Delta\boldsymbol{\lambda}\right) = -\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) = -\mathcal{L}\bar{\boldsymbol{\lambda}} - \mathcal{L}\Delta\bar{\boldsymbol{\lambda}} \tag{7.11}$$

The above cyber layer demonstrates that the controller is able to establish one consensus value and achieve steady state while being under attack. However, this consensus value is now based on combining the consensus value of the incremental costs of each DG and additional attacked values $\Delta\boldsymbol{\lambda}$. The control objective *1* is therefore not satisfied. Additionally, as the steady state operations now depends on establishing consensus for the two vectors $\boldsymbol{\lambda}$ and $\Delta\boldsymbol{\lambda}$ it will take longer time to cooperative define the consensus values and achieve the desired steady state. Hence, even though the cyber controller is able to achieve consensus, the value will be of false high values when the attacks are intruding the communication links and the control objective *1* is not achieved at the steady state equilibrium. The cooperatively established operating value is not equal to the optimal consensus value corresponding to the equal incremental costs of generation.

By studying the dynamics and applying the resilient controller strategy proposed in *Hypothesis* 1, it is observed that tuning of $\boldsymbol{\alpha}$ to a significant high value will remove the effect of the attack. The consensus value will be defined by only communicated incremental costs of each DG. The attack adding false values, $\Delta\boldsymbol{\lambda}$, does not have any effect when the resilient control strategy is applied as $\boldsymbol{\lambda} = 2\boldsymbol{\alpha}\mathbf{I}^{\mathcal{G}} + \boldsymbol{\beta}$ will be significantly greater than the attack value. The controller is then able to ensure the optimal consensus value and the equal incremental costs control objective is satisfied at the steady state equilibrium while the system is subject to cyber attacks.

The second control objective is then assessed at the new equilibrium of the physical network. The disturbed secondary controller is first expressed at the equilibrium:

$$\bar{\mathbf{u}}_{tot} = \mathbf{R}^D \bar{\mathbf{I}}^{\mathcal{G}} - K_p \mathbf{w}^{-1} \mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) + \mathbf{w}^{-1} \mathcal{L} \mathbf{K}_I (\bar{\mathbf{x}}_c + \Delta\bar{\mathbf{x}}_c) \tag{7.12}$$

Second, this $\bar{\mathbf{u}}_{tot}$ is replaced in the voltage-current droop/primary control equation: $\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D \bar{\mathbf{I}}^{\mathcal{G}} + \bar{\mathbf{u}}_{tot}$. By adding the weightings of the individual DGs, the voltage control is represented below at the new equilibrium.

$$\mathbf{1}^\top \mathbf{w} \bar{\mathbf{V}} = \mathbf{1}^\top \mathbf{w} \mathbf{1} V_{nom} + \mathbf{1}^\top \mathbf{w} \left[ -K_p \mathbf{w}^{-1} \mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) \right] + \mathbf{1}^\top \mathbf{w} \mathbf{w}^{-1} \mathcal{L} \mathbf{K}_I (\bar{\mathbf{x}}_c + \Delta\bar{\mathbf{x}}_c) \tag{7.13}$$

We arrive at the final equation for the average voltage regulation, defined below, by using the property of the Laplacian where $\mathbf{1}^\top \mathcal{L} = 0$.

$$\mathbf{1}^\top \mathbf{w} \bar{\mathbf{V}} = \mathbf{1}^\top \mathbf{w} \mathbf{1} V_{nom} \tag{7.14}$$

Hence, it is proven that the system ensures that the weighted sum of all the DG's voltages is are equal to the predefined nominal voltage $V_{nom}$ even when the system is under attack in the communication links. When the resilient control strategy is tested on the new equilibrium, the above equation shows that the tuning of $2\boldsymbol{\alpha} = \mathbf{w}^{-1}$ will only scale the voltages and not disturb the ability to achieve the desired average voltage regulations.

## 7.5 Simulations of Attacked System

In order to simulate the potential cyber attacks in the communication links, the attack vectors $\Delta\boldsymbol{\lambda}$ and $\Delta\mathbf{x}_c$ are implemented as constant–and time varying–intrusions to the case specific MG. Even though the Laplacian is defined as undirected the attack vectors intruding the MG needs to be implemented with respect to the arbitrary but defined Laplacian matrix previously established in 2.8 in *Part A*. The dynamics of the case specific distributed control network are given below.

$$DG1: \begin{cases} u_{tot,1} = R_1^D I_1^{\mathcal{G}} + 2\alpha_1 (K_p z_1^{*\lambda} - z_1^{*c}) \\ \dot{x}_1^c = z_1^{*\lambda} \\ z_1^{*\lambda} = (\lambda_2 - \lambda_1) + \Delta\lambda_2 \\ z_1^{*c} = K_1^I \left[ (x_2^c - x_1^c) + \Delta x_2^c \right] \\ \lambda_1 = 2\alpha_1 I_1^{\mathcal{G}} + \beta_1 \end{cases} \qquad DG2: \begin{cases} u_{tot,2} = R_2^D I_2^{\mathcal{G}} + 2\alpha_1 (K_p z_1^{*\lambda} - z_1^{*c}) \\ \dot{x}_1^c = z_1^{*\lambda} \\ z_2^{*\lambda} = (\lambda_1 + \lambda_3 \lambda_4) - 3\lambda_2 \\ \qquad + (\Delta\lambda_1 + \Delta\lambda_3 + \Delta\lambda_4) \\ z_2 * c = K_2^I \left[ (x_1^c + x_3^c + x_4^c) - 3x_2^c \right. \\ \qquad \left. + (\Delta x_1^c + \Delta x_3^c + \Delta x_4^c) \right] \\ \lambda_2 = 2\alpha_2 I_2^{\mathcal{G}} + \beta_2 \end{cases} \tag{7.15}$$

$$DG3: \begin{cases} u_{tot,3} = R_3^D I_3^{\mathcal{G}} + 2\alpha_3 (K_p z_3^{*\lambda} - z_3^{*c}) \\ \dot{x}_3^c = z_3^{*\lambda} \\ z_3^{*\lambda} = (\lambda_2 + \lambda_4) - 2\lambda_3 + (\Delta\lambda_2 + \Delta\lambda_4) \\ z_3^{*c} = K_3^I \left[ (x_2^c + x_4^c) - 2x_3^c + (\Delta x_2^c + \Delta x_4^c) \right] \\ \lambda_3 = 2\alpha_3 I_3^{\mathcal{G}} + \beta_3 \end{cases} \qquad DG4: \begin{cases} u_{tot,4} = R_4^D I_4^{\mathcal{G}} + 2\alpha_4 (K_p z_4^{*\lambda} - z_4^{*c}) \\ \dot{x}_4^c = z_4^{*\lambda} \\ z_4^{*\lambda} = (\lambda_2 + \lambda_3) - 2\lambda_4 + (\Delta\lambda_2 + \Delta\lambda_3) \\ z_4^{*c} = K_4^I \left[ (x_2^c + x_3^c) - 2x_4^c + (\Delta x_2^c + \Delta x_3^c) \right] \\ \lambda_4 = 2\alpha_4 I_4^{\mathcal{G}} + \beta_4 \end{cases} \tag{7.16}$$

The simulations of the system prone to cyber attacks in the communication links, are based on the previously tested unforced system presented in *Part A* Section 4. The attack vector infiltrating the communicated incremental costs is implemented with values $\Delta\boldsymbol{\lambda} = [10, 3, 8, 0]^\top$ and the attack perturbing the controller states is implemented as $\Delta\mathbf{x}_c = [1, 15, 0, 3]^\top$. The attacks are starting to add false values to the communicated values at 5 seconds and vanished at 20 seconds. The events simulated for the unforced system is still implemented in order to see the system response for regular system changes in addition to the cyber attacks and the untuned control parameters are given in Table 4.2. Figure 7.3 and 7.4 represents the system response of the proposed case specific MG with the simulated attacks. The tuning of the controller is not yet conducted and the figures simulates the system response for the proposed PI-controller.

Figure 7.2: Perturbed MG under CA3

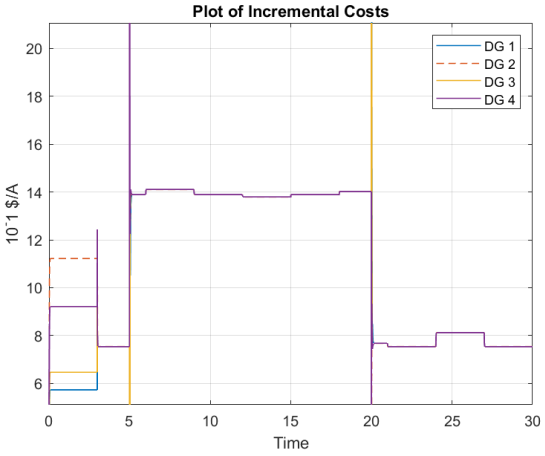


Figure 7.3: Incremental costs of perturbed system

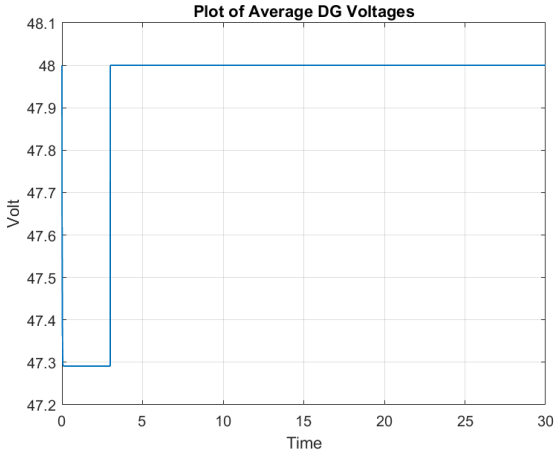


Figure 7.4: Average voltage of perturbed system

As explained in the above mathematical proof, the time to achieve consensus may be longer due to the attack. Subsequently it takes longer time to achieve steady state and the figures below showcases this time to achieve consensus and steady state when the attack is perturbing, vanishing and when the inherent system changes takes place. Figure 7.6 shows that the consensus is not ensures at 5 seconds: i.e., the time when the attack is intruding in the communicated values and it is observed that the controller uses some time to cooperatively define the consensus value. Figure 7.7 and 7.8 shows the system response at respectively 12 and 20 second: i.e., when the current is decreased at load four and when the attack is vanishing. The same conclusion is drawn: i.e., this system is able to operate as stable, however uses longer time to achieve consensus.

Figure 7.5: Perturbed MG under CA3

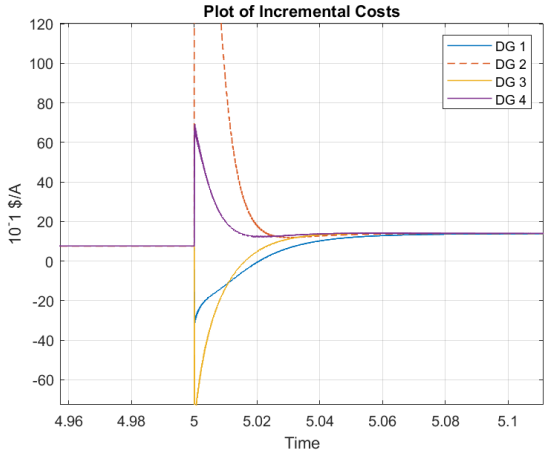


Figure 7.6: Incremental costs of perturbed system, at 5 seconds

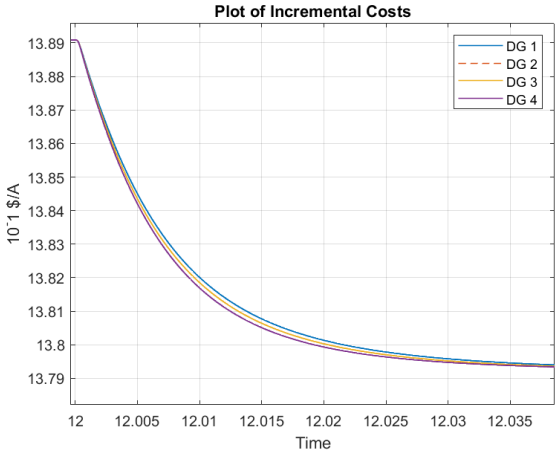


Figure 7.7: Incremental costs of perturbed system, at 12 seconds

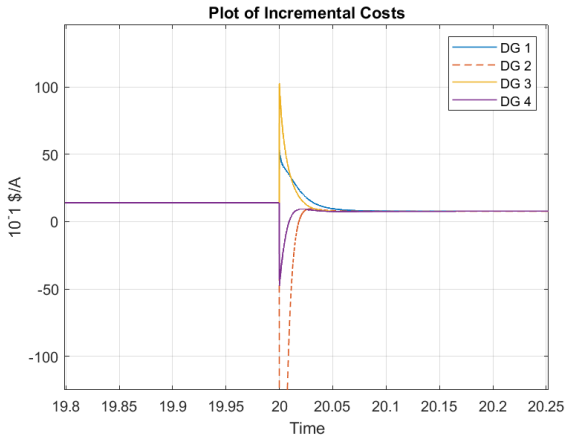


Figure 7.8: Incremental costs of perturbed system, at 20 seconds

The simulations are now conducted with the primary control parameter tuned to minimum tuning value 3000 established in *Appendix* B, testing the proposed resilient control strategy. Figure 7.10 shows that the system response is approximately operating as the unforced system. Figure 7.11 shows the system is able to achieve consensus in $\approx 0,025$ seconds. For comparisons, the controller without tuning used $\approx 0,08$ seconds. Hence, the time to achieve consensus and steady state is significantly faster with the resilient control strategy.

Figure 7.9: Primary Control Parameter Tuned to 3000

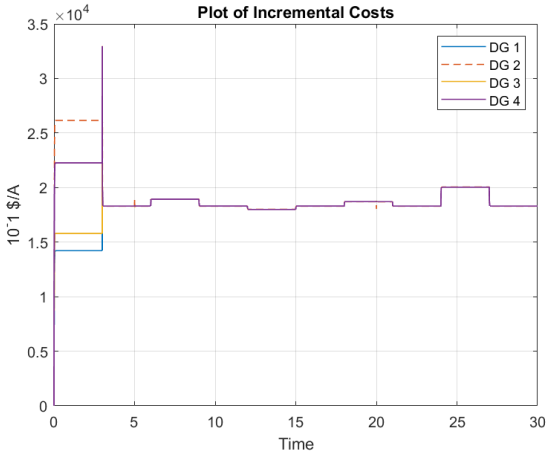


Figure 7.10: Incremental costs of perturbed system, with primary controller tuned to 3000

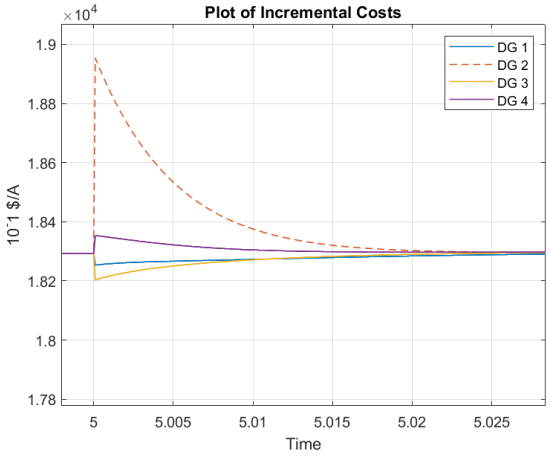


Figure 7.11: Incremental costs of perturbed system, with primary controller tuned to 3000, at 5 seconds

The performance of the controller is show even more sufficient by comparing the time to achieve consensus when the integrator gain $\mathbf{K}_I$ is reduced from 100 to 10 (only performed for the two subsequent figures). In Figure 7.12 the controller is not yet tuned and the time to achieve consensus is $\approx 1$ second. When the controller is tuned to 3000 presented in Figure 7.13 the consensus time is $\approx 0.25$ seconds, showing that the resilient controller sufficiently removes the influence of the attack while ensuring steady state in less time.

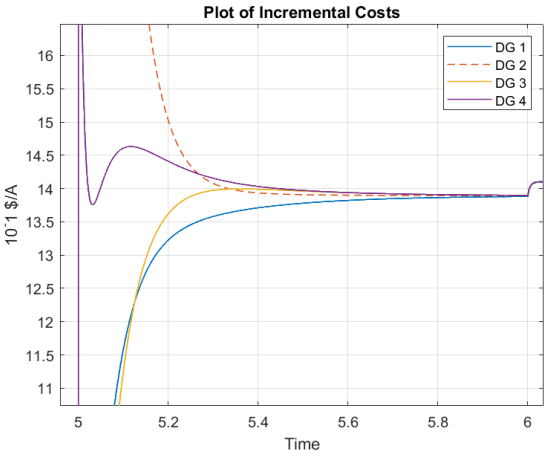


Figure 7.12: Incremental costs of perturbed system, without resilient tuning, at 5 seconds

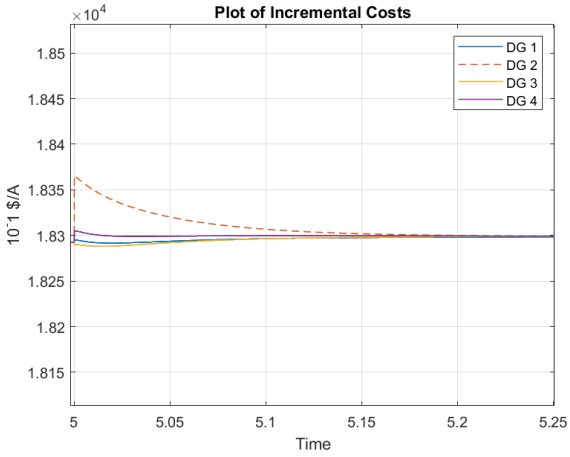


Figure 7.13: Incremental costs of perturbed system, with resilience equal to 3000, at 5 seconds

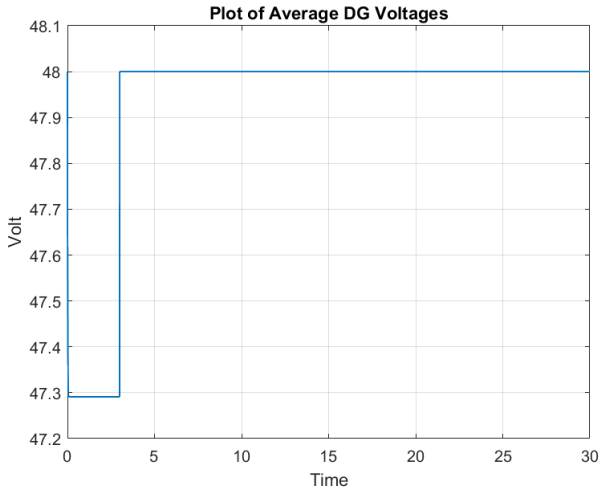


Figure 7.14: Average voltage of perturbed system, with resilience equal to 3000

Figure 7.14 shows the system's average voltage response when the primary controller is tuned to 3000. It is therefore shown in the simulations that the tuning of $\boldsymbol{\alpha}$ increases the ability to ensure optimal consensus values at the steady state equilibrium while the system is under attack, and to not change the ability to maintain average voltage regulation. The proposed resilient control strategy is therefore observed sufficient in ensuring the two control objectives.

**Time Varying Cyber Attacks**

As previously explained the cyber attacks may be of constant values or time varying values. When the attacks are constants, they will disappear mathematically when the system is brought to the incremental level as the constants are of equal values at the present operational state and the desired equilibrium state. Hence, they are cancelled out due to the definition of incremental energy. However, when the cyber attacks are intruding as continuous and time varying perturbations, the attack vectors will have values at the incremental level as implemented in the defined Lyapunov function. It is therefore interesting to additionally simulate a time varying cyber attack in the communication links and see the system responses.

The attack vectors are now implemented as $\Delta\boldsymbol{\lambda}(t) = [5 \cdot sin(t), 3, 8, 0]^\top$ and $\Delta\mathbf{x}_c = [1, 15, 0, 3]^\top$. Figure 7.15 and 7.16 presents the incremental costs and the average voltage response of the system with untuned control parameters. Figure 7.15 shows that the controller ensures consensus. However, it is observed that the time varying perturbation brings the system to operate further away from the desired operations presented for the unforced system. Figure 7.16 presents that the system is able to ensure average voltage regulation even with time varying perturbations.

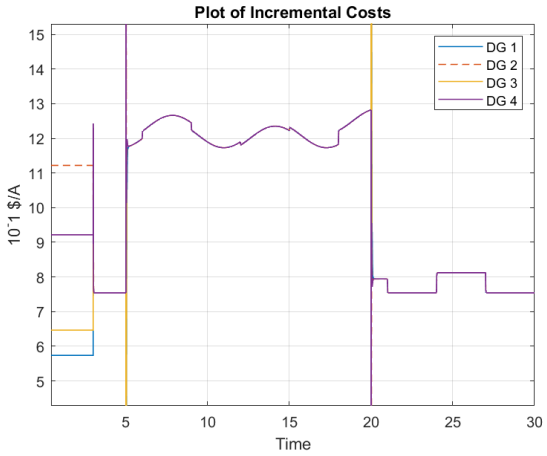


Figure 7.15: Incremental costs of time varying perturbed system, without resilience

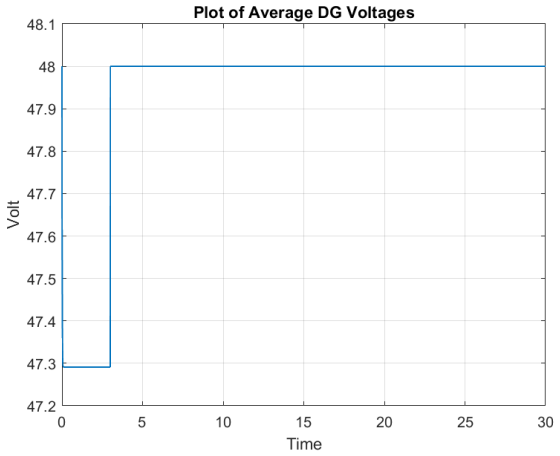


Figure 7.16: Average voltage of time varying perturbed system, without resilience

The same time varying cyber attack $\Delta\boldsymbol{\lambda}(t)$ is now simulated with the tuned $\boldsymbol{\alpha}$ equal to 3000. Figure 7.17 presents the same system response as Figure 7.10 and the resilient controller is proven sufficient even with time varying perturbations. This is also validated in the above sections. The Figure below shows that average voltage will be unchanged with regards to the control parameter tuning, as also previously concluded.

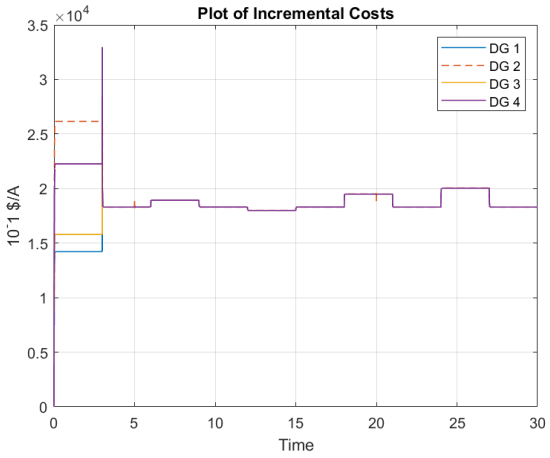


Figure 7.17: Incremental costs of time varying perturbed system, with resilience equal to 3000

## 7.6 Conclusion of the System Analysis while Subject to Cyber Attack 3

In the above sections it is proven that the system converges to ISS stability bounded by the two potential bounded attacks, $\Delta\boldsymbol{\lambda}$ and $\Delta\mathbf{x}_c$. The steady state operating point is established within the bound of the attacks, ensuring that the system converges to the closest neighbouring equilibrium to the desired equilibrium. The properties of the secondary controller is then tested at this new established equilibrium and it is proven that the system is able to ensure average voltage regulation while being under attack in the communication links. This is due to the fact that the attack intrudes between the units in the cyber layer and when the secondary control input is delivered to the electrical layer, the influence of the attack is removed due to the communication matrix, $\mathcal{L}$. When the new equilibrium on the control network is studied, assessing if the units are able to cooperatively establish a consensus value of the incremental costs, the controller fails to perform optimally. The units will agree upon two established cooperative values, due to the dynamics of the controller. However, the final consensus value is then based on the two communicated values, $\boldsymbol{\lambda}$ and $\Delta\boldsymbol{\lambda}$, and the final consensus value will not correspond to the optimal consensus value: i.e., the cooperatively obtained equal incremental cost value. Additionally, the controller uses longer time to reach steady state operations. This brings the system to work as compromised during the attack.

In *Part B* Section 1 the resilient controller was proposed, assuming capable to eliminate the attack by tuning the primary control parameter to a significant high value. By studying the equilibrium of the cyber layer it has been shown, mathematically and validated by simulations, that tuning of $\boldsymbol{\alpha}$ is sufficient in order to ensure optimal incremental costs while the system is under attack. It is also concluded that the high primary control parameter will not affect the performance of the voltage controller. The final conclusion is therefore that the *Hypothesis* 1 is a sufficient resilient control strategy, bringing the system to operate as unforced while being under attack in the communication links. The controller is also concluded sufficient and robust against both the continuous and time varying attacks.

## Part C:

# Cyber Attack Resilient Control Modifications

*Part B* of this thesis analyses how three different cyber attacks influence the perturbed systems when intruding in different locations of the control system. Influenced by Mahdieh S. Sadabadi, the first resilient control strategy was implemented on the control system – influenced by Babak Abdolmaleki's publication [1] – as a novel and adaptive controller able to operate the MG as close to the desired equilibrium as possible while being under attack. It was assumed that the resilience property was achieved when tuning the control parameter $\boldsymbol{\alpha}$ to significant high values. However, the dynamical equations at the equilibrium of the forced microgrid shows that the high control parameter only is able to robustify the control with respect to the first control objective for some cyber attacks. Motivated by this shortcomming, *Part C* of this thesis will therefore modify the control system and establish a new resilient control strategy in order to additionally comply with the second control objective. The intention of this modification is then to ensure that the system is able to operate as if it was not being subject to any attacks: i.e., both control objectives are achieved while the system is under attack and thereby satisfy the third control objective: *resilience against cyber threats*. This new resilient controller is then tested for the three cyber attacks under consideration, ensuring that the control objectives are fulfilled regardless of where the attack intrudes.

# 1 Proposition of Control Modifications

By increasing the value of the control parameter $\alpha$ the consensus property is improved at the equilibrium, however improving the average voltage regulation. Motivated by this shortcoming, a new control modification is proposed in this section, focusing on regulating the average voltage to a desired reference, even when the system is subject to cyber attacks. More precisely, the intention is to establish a second control parameter, $\zeta$, that is able to remove the effect of the cyber attack if tuned appropriately. The first cyber attack studied in this thesis, was the FDIA infiltrating in the control actuators. The voltage control objective was not satisfied at the new equilibrium as the weighted voltage were previously given as:

$$\mathbf{1}^\top \mathbf{w}\bar{\mathbf{V}} = \mathbf{1}^\top \mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top \mathbf{w}\Delta\bar{\mathbf{u}} \tag{1.1}$$

By tuning the primary control parameter $\boldsymbol{\alpha}$ to high values, it is displayed that the influence of the attack is rather amplified than removed due to the relation $\mathbf{w} = \frac{1}{2\boldsymbol{\alpha}}$. The secondary control parameter $\zeta$ is therefore added to the control dynamics in order mitigate the influence of the attack. $\zeta$ is defined in 1.2 implemented as a scalar value used as a gain at the defined suitable locations in the secondary controller.

$$\zeta \triangleq \frac{1}{\mu} \tag{1.2}$$

Studying the forced voltage control equation in 1.1 in *Part B* shows that adding the secondary control parameter in front of the attack will reduce the effect of the attack proportionally with high tuning of $\mu$. The first step is then to decide where the secondary control parameter needs to be added so that $\zeta$ always will appear in front of any potential attack without intruding the performance of other system dynamics.

As previously defined, the cyber attacks may intrude the distributed controller due to the use of communication links: i.e., sharing values online and cooperatively establishing the desired optimal operations. Consequently, the average voltage regulation is only disturbed when the attack appears in the distributed control network at the locations where the secondary controller is defined as the voltage regulating unit. $\mathbf{u}_{tot}$ and the new control parameter is therefore added in the voltage control dynamics: $\mathbf{V}^{\mathcal{G}} = \mathbf{V}^{ref} = \mathbf{V}_{nom} - \mathbf{R}^{\mathcal{D}}\mathbf{I}^{\mathcal{G}} + \zeta\mathbf{u}_{tot}$. This will guarantee that the potential attack – perturbing the voltage regulation – always will be multiplied with $\zeta$, and it is therefore possible to tune the control parameter and remove the attack influence with respect to the voltage control objective.

When the secondary control parameter is added, the rest of the system dynamics needs to be assessed ensuring that the added parameter does not change the behaviour of other dynamics. The secondary controller is modelled, cancelling out the primary droop control the DGs. However, when the new control parameter is multiplied, the droop is not cancelled as desired. The proposed passivity based PI- controller $\mathbf{r}$ needs to be modified so that the system is only controlled by the secondary controller: i.e., completely cancel out the droop. The proposed modified controller is formally defined in *Definition* 2.

**Definition: 2.** *The secondary control parameter $\zeta$ is added in the voltage control: $\mathbf{V}^{\mathcal{G}} = \mathbf{V}_{nom} - \mathbf{R}^{\mathcal{D}}\mathbf{I}^{\mathcal{G}} + \zeta\mathbf{u}_{tot}$. The PBC PI-controller is given the dynamics: $\mathbf{r}_{new} = -\frac{1}{\zeta}\mathbf{R}^{D} + K_p\mathbf{w}^{-1}\mathcal{L}\mathbf{w}^{-1}$ where $K_p > 0$ and $\zeta = \frac{1}{\mu} > 0$*

The final resilient controller is then presented below, as a combination of *Hypothesis* 1 and the proposed control modification defined in *Definition* 2.

**Hypothesis: 2.** *The resilience is ensured when tuning both the primary control parameter $\boldsymbol{\alpha}$ and the secondary control parameter $\mu$ to significant high values, removing the effect of the perturbation term and establishing a resilient controller robust against all cyber attacks.*

The additional assumption presented in *Assumption* 2 is equally important when *Hypothesis* 2 is validated. It is worth recalling at this point that the *Assumption* 2 assumes that $\boldsymbol{\alpha} > 0$. Additionally it is recognized that the adding of the scalar secondary control parameter will not influence *Assumption* 1. Hence, the interconnected unforced CP MG is still assumed to have an equilibrium facilitating the later applied incremental energy modelling.

# 2 Linear System Representation

The next step is then to analyse this new proposed controller for the previously studied forced systems. The unforced linear system is firstly established with the modified control system, defined as the base case used in

all the subsequently system analysis. *Definition* 2 includes adding the new control parameter to the control dynamics of the electrical system. Hence, the modified electrical dynamics are presented below:

$$L_i^{\mathcal{G}} \dot{I}_i^{\mathcal{G}} = V_i^{\mathcal{G}} - \sum_k b_{ki}^{\mathcal{G}} V_k^{\mathcal{N}} - R_i^{\mathcal{G}} I_i^{\mathcal{G}} \tag{2.1}$$

$$L_j^{\mathcal{E}} \dot{I}_j^{\mathcal{E}} = -\sum_k b_{kj}^{\mathcal{E}} V_k^{\mathcal{N}} - R_j^{\mathcal{E}} I_j^{\mathcal{E}} \tag{2.2}$$

$$\mathcal{C}_k^{\mathcal{N}} \dot{V}_k^{\mathcal{N}} = \sum_j b_{kj}^{\mathcal{E}} I_j^{\mathcal{E}} + \sum_i b_{ki}^{\mathcal{G}} I_i^{\mathcal{G}} - I_k^L \tag{2.3}$$

$$I_k^L = G_k^{cte} V_k^{\mathcal{N}} + I_k^{cte} \tag{2.4}$$

$$V_i^{\mathcal{G}} = V_i^{ref} = V_{nom} - R_i^{\mathcal{D}} I_i^{\mathcal{G}} + \zeta u_{tot} \tag{2.5}$$

The closed loop control system is then establish with the new interconnection pattern:

$$\begin{aligned} \begin{bmatrix} \mathbf{u}_{tot} \\ \mathbf{u}_c \end{bmatrix} &= \begin{bmatrix} -\mathbf{r}_{new} & -(\mathbf{w}^{-1}) \\ (\mathbf{w}^{-1})^\top & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ \mathbf{b}_c \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\zeta}\mathbf{R}^D - K_p 2\boldsymbol{\alpha}\mathcal{L}2\boldsymbol{\alpha} & -(2\boldsymbol{\alpha}) \\ (2\boldsymbol{\alpha})^\top & 0 \end{bmatrix} \begin{bmatrix} \mathbf{y}_{tot} \\ \mathbf{y}_c \end{bmatrix} + \begin{bmatrix} -K_p 2\boldsymbol{\alpha}\mathcal{L}\boldsymbol{\beta} \\ \boldsymbol{\beta} \end{bmatrix} \end{aligned} \tag{2.6}$$

The constants are unaltered, still defined as: $\mathbf{b} = -K_p \mathbf{w}^{-1}\mathcal{L}\boldsymbol{\beta}$ and $\mathbf{b}_c = \boldsymbol{\beta}$. The weightings remains equal to $2\boldsymbol{\alpha}$ and they are still necessary in the new control system. Notice that the new modification is not meant to change the ability of the controller to reach the control objective when unforced. The weightings are therefore still used to guarantee both voltage control and consensus, as later explained in detail. With the above closed loop configurations the inherent dynamics of the distributed controller is expressed in scalar form as below.

$$\begin{cases} u_{tot} = \frac{1}{\zeta} R_i^D I_i^{\mathcal{G}} + 2\alpha_i (K_p z_i^\lambda - z_i^c) \\ \dot{x}_i^c = z_i^\lambda \\ z_i^\lambda = \sum_{j \in \mathcal{N}_c} a_{ij}(\lambda_j - \lambda_i) \\ z_i^c = \sum_{j \in \mathcal{N}_c} a_{ij} K_i^I (x_j^c - x_i^c) \\ \lambda_i = 2\alpha_i I_i^{\mathcal{G}} + \beta_i \end{cases} \tag{2.7}$$

When the secondary control parameter $\zeta$ is implemented, the interconnected linear pH system representation is given in 2.8.

$$\begin{bmatrix} \dot{\boldsymbol{\phi}}^{\mathcal{G}} \\ \dot{\boldsymbol{\phi}}^{\mathcal{E}} \\ \dot{\mathbf{q}}^{\mathcal{N}} \\ \dot{\mathbf{x}}^c \end{bmatrix} = \begin{bmatrix} \left[\zeta 2\boldsymbol{\alpha}(-K_p \mathcal{L} 2\boldsymbol{\alpha}) - \mathbf{R}^{\mathcal{G}}\right] & 0 & \left[-\mathcal{B}^{\mathcal{G}\top}\right] & [\zeta 2\boldsymbol{\alpha}\mathcal{L}] \\ 0 & \left[-\mathbf{R}^{\mathcal{E}}\right] & \left[-\mathcal{B}^{\mathcal{E}\top}\right] & 0 \\ \left[\mathcal{B}^{\mathcal{G}}\right] & \left[\mathcal{B}^{\mathcal{E}}\right] & \left[-\mathbf{G}^{cte}\right] & 0 \\ [-\mathcal{L}2\boldsymbol{\alpha}] & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{I}^{\mathcal{G}} \\ \mathbf{I}^{\mathcal{E}} \\ \mathbf{V}^{\mathcal{N}} \\ \boldsymbol{\eta}^c \end{bmatrix} \tag{2.8}$$

# 3 Energy and Stability Analysis

For the sake of completeness the energy and stability analysis of the base case, with the modified controller, is presented. Even though it is arguably reasonable to assume that adding a scalar gain will not disturb the preserved energy and the stability results of the system, it is still useful to replicate the proof in order to complete the Lyapunov stability analyses–including those under the different types of attack.

The proposed Lyapunov candidate, with the new secondary control parameter $\zeta$, is based on the Hamiltonian of the system and will therefore be based on how the energy is stored and preserved within the network. By studying the new **A**-matrix presented in 2.8 it can be observed that the skew-symmetric properties are not uphold as the matrix element $A_{14} \neq -A_{41}^\top$. This is due to the added control parameter $\zeta$ and the Lyapunov function needs to be modified to take this into account. This is important as the power preservation: i.e., skew-symmetric properties of the pH system representation is a useful property when finding a Lyapunov function and assessing the stability. Fortunately, since $\zeta$ is a scalar, this additional challenge can be easily overcome by scaling the cyber energy in the Lyapunov function candidate with the value of $\zeta$. This will ensure the necessary properties of the proposed storage function so that $\dot{V}(\tilde{x}) \leq 0$ and the Lyapunov candidate is defined as the stability certificate for the final system.

In order to obtain the Lyapunov candidate the same approach as previously used, is presented in this section. First, the Hamiltonian of the MG with the secondary control parameter is defined as:

$$\begin{aligned} H_T(x_T) &= H_{tot}(x_{tot}) + H_c(x_c) \\ &= \frac{1}{2}\mathbf{x}_{tot}^\top \mathbf{Q}_{tot}\mathbf{x}_{tot} + \frac{1}{2}\mathbf{x}_c^\top \mathbf{K}_I \mathbf{x}_c \end{aligned} \tag{3.1}$$

By studying the previously defined Hamiltonians, it is shown that the stored energy does not change either with the added cyber attacks or with the new modified control. However, the change in stored energy will be changed as the secondary controller delivered to the physical network, $\mathbf{u}_{tot}$, will be scaled with the secondary control parameter $\zeta$. The time-dependent energy flows is then expressed below.

$$\begin{aligned} \dot{H}_T(x_T) &= \dot{H}_{tot}(x_{tot}) + \dot{H}_c(x_c) \\ &= \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{F}_{tot}\boldsymbol{\nabla}H_{tot}(x_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{g}_i^{\mathcal{G}}\zeta\mathbf{u}_{tot}^{\mathcal{G}} + \boldsymbol{\nabla}^\top H_{tot}(x_{tot})\mathbf{E}_{tot} + \boldsymbol{\nabla}^\top H_c(x_c)\mathbf{g}_c\mathbf{u}_c \end{aligned} \tag{3.2}$$

The next step in the Lyapunov stability analysis is to establish the proposed storage function influenced by the Hamiltonian, based on the incremental states, and by scaling the cyber energy ensuring the skew-symmetry of the unforced system. The Lyapunov candidate is then defined as:

$$V_T(\tilde{x}_T) = H_{tot}(\tilde{x}_{tot}) + \zeta H_c(\tilde{x}_c) \tag{3.3}$$

Taking its time-derivative gives:

$$\begin{aligned} \dot{V}_T(\tilde{x}_T) &= \dot{H}_{tot}(\tilde{x}_{tot}) + \zeta\dot{H}_c(\tilde{x}_c) \\ &= -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{R}_{tot}\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\zeta\tilde{\mathbf{u}}_{tot}^{\mathcal{G}} + \zeta\boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\tilde{\mathbf{u}}_c \end{aligned} \tag{3.4}$$

It is now assessed if this new Lyapunov function will have similar power preserving properties than its predecessor, yet with the modified controller. Studying the closed loop control system in 2.6, and the lossy skew-symmetric properties are defined at the incremental level as: $\tilde{\mathbf{u}}_{tot} = -\mathbf{r}_{new}\tilde{\mathbf{y}}_{tot} - \mathbf{w}^{-1}\tilde{\mathbf{y}}_c$ and $\tilde{\mathbf{u}}_c = \mathbf{w}^{-1^\top}\tilde{\mathbf{y}}_{tot}$. By using this lossy skew-symmetry and the previously defined energy changes outputs of each network, term two and three of the Lyapunov candidate time-derivative are expressed as:

$$\begin{aligned} \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\zeta\mathbf{g}_i^{\mathcal{G}}\tilde{\mathbf{u}}_{tot} &= \mathbf{y}_{tot}^\top\zeta\tilde{\mathbf{u}}_{tot} \\ &= \tilde{\mathbf{y}}_{tot}^\top\zeta(-\mathbf{r}_{new}\tilde{\mathbf{y}}_{tot} - \mathbf{w}^{-1}\tilde{\mathbf{y}}_c) \end{aligned} \tag{3.5}$$

$$\begin{aligned} \zeta H_c(\tilde{x}_c)\mathbf{g}_c\tilde{\mathbf{u}}_c &= \zeta\tilde{\mathbf{y}}_c^\top\tilde{\mathbf{u}}_c \\ &= \zeta\tilde{\mathbf{y}}_c^\top(\mathbf{w}^{-1^\top}\tilde{\mathbf{y}}_{tot}) \end{aligned} \tag{3.6}$$

From previous definitions the scaled controller $\zeta\mathbf{r}$ is implemented in the final dissipation matrix, $\mathbf{T}_T$. It is then shown that term number two and three are canceling out due to the scalar $\zeta$ implemented as a scaling factor for the cyber energy. Hence, $-\zeta\tilde{\mathbf{y}}_{tot}^\top\mathbf{w}^{-1}\tilde{\mathbf{y}}_c + \zeta\tilde{\mathbf{y}}_c^\top\mathbf{w}^{-1^\top}\tilde{\mathbf{y}}_{tot} = 0$ and we have ensured power preservation between the two networks (i.e., the physical and the cyber layers), arriving at the final Lyapunov function expressed 3.7. This function is then used as the stability certificate as it proves the global asymptotic stability of the system, previously explained in associated specialization project presented in *Appendix* D and in *Part B* Section 5.3.2. The Lyapunov function ensures that the energy decreases to the equilibrium when time goes to infinity and the system is proven stable at the equilibrium point of the cyber-physical microgrid with the modified controller.

$$\dot{V}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) \leq 0 \tag{3.7}$$

**Lyapunov Stability Certificates**

The Lyapunov stability certificates are previously obtained in the stability assessment of the perturbed systems prone to the three different cyber attacks. The final Lyapunov functions are all depending on the dissipation within the electrical network and reduced/increased energy due to the bounded cyber attacks. When the new secondary control parameter is added as a constant scaling coefficient as presented in *Hypothesis* 2, the cyber energy also needs to be scaled in the Lyapunov function in order to ensure power preservation, as explained for the unforced system. The three Lyapunov functions for the forced systems are given below where the scaled

secondary controller and scaled cyber energy are implemented.

$$\text{Cyber Attack 1:} \quad \dot{V}_T(\tilde{x}_T) = -\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) + \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\zeta\Delta\check{\mathbf{u}} \tag{3.8}$$

$$\begin{aligned}\text{Cyber Attack 2:} \quad \dot{V}_T(\tilde{x}_T) = &-\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\zeta\mathbf{r}\Delta\tilde{\mathbf{I}} \\ &+ \zeta\boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\mathbf{w}^{-1}\Delta\tilde{\mathbf{I}}\end{aligned} \tag{3.9}$$

$$\begin{aligned}\text{Cyber Attack 3:} \quad \dot{V}_T(\tilde{x}_T) = &-\boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{T}_T\boldsymbol{\nabla}H_{tot}(\tilde{x}_{tot}) - \boldsymbol{\nabla}^\top H_{tot}(\tilde{x}_{tot})\mathbf{g}_i^{\mathcal{G}}\zeta\left(\mathbf{r}_1\Delta\tilde{\boldsymbol{\lambda}} + \mathbf{r}_2\Delta\tilde{\mathbf{x}}_c\right) \\ &+ \zeta\boldsymbol{\nabla}^\top H_c(\tilde{x}_c)\mathbf{g}_c\Delta\tilde{\boldsymbol{\lambda}}\end{aligned} \tag{3.10}$$

The above time-derivatives of the Lyapunov functions shows that the system is *input-to-state stable*; i.e., if the attack is removed, the system converges to its equilibrium–for all three attacks. Moreover, this property also implies (for linear systems) that the states will be bounded if the attack is bounded. Furthermore, when $\mu$ is tuned to a significant high value, it is actually shown that the terms related to the attack can be significantly mitigated as $\zeta = \frac{1}{\mu}$ and all the terms with the multiplied $\zeta$ will tend to zero and the systems achieve global exponential stability.

The above energy and stability assessment concludes that the perturbed systems achieves ISS regardless of the potential attacks, as also defined in *Lemma 4.5* in the Khalil's book Nonlinear Control [23]. This is an important property of the resilient control design as the goal is to design a controller that ensured stability regardless of the type of attack.

# 4 Approach to Analyse modified controller

In the next sections of this thesis the three cyber attacks under consideration are again analysed as potential disturbances that may perturbs the operations of the MG. The unforced cyber-physical MG with the modified controller, presented in *Part C* Section 2, is now used as the base case when the potential attacks are studied.

It is already proven that both the unforced system and the systems subject to the three attacks are able to converge to a new equilibrium point as they are all defined exponentially stable or ISS. It is therefore necessary to assess those new equilibrium points with respect to the two desired control objectives with the modified control system. The equilibrium points are subsequently assessed under the assumption that significant high primary control parameters $\boldsymbol{\alpha}$ and high secondary control parameter $\mu$ will decrease the influence of the attacks, bringing the system to operate as close to the equilibrium of the unforced system as possible. The three cyber attacks are also simulated with the modified controller with regular control parameters and scaled parameters to see the effect of the proposed controller, wanting the MG to operate as an unforced system while being under attack.

# 5 Cyber Attack 1: Equilibrium Analysis

The performance of the modified controller is now assessed at the equilibrium while the system is under attack in the actuators of the controller. In the previous analysis of this attack, with only $\boldsymbol{\alpha}$ as the proposed resilient control parameter, it was shown that the controller was able to ensure the equal incremental cost control objective but no weighted average voltage regulation at the new equilibrium. With the new modified controller, the equilibrium analysis is re-conducted analysing if the controller is able to ensure both of the control objectives at the equilibrium point with the appropriate tuning of $\boldsymbol{\alpha}$ and $\mu$. The equilibrium of the distributed control network is defined as in *Part B* Section 5.2, however the secondary control parameter needs to be added and the two modified controllers are given as:

$$\begin{aligned}\bar{\mathbf{u}}_{tot} &= \frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(K_p\mathbf{z}^\lambda - \mathbf{z}^c) + \Delta\bar{\mathbf{u}} \\ &= \frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\boldsymbol{\lambda}} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}}\end{aligned} \tag{5.1}$$

$$\bar{\mathbf{u}}_c = 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot} + \boldsymbol{\beta} = 2\boldsymbol{\alpha}\bar{\mathbf{I}}^{\mathcal{G}} + \boldsymbol{\beta} = \bar{\boldsymbol{\lambda}} \tag{5.2}$$

Average voltage regulation was the problematic objective when the system was subject to cyber attacks in the control actuators, and is therefore firstly assessed. The voltage control at the equilibrium point with the new

control system is expressed as $\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \zeta\bar{\mathbf{u}}_{tot}$. By implementing the new secondary controller defined in 5.1, the final voltage control is expressed as:

$$\begin{aligned}\bar{\mathbf{V}} &= \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \zeta\left[\frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\boldsymbol{\lambda}} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \Delta\bar{\mathbf{u}}\right] \\ &= \mathbf{1}V_{nom} + \zeta 2\boldsymbol{\alpha}(-K_p\mathcal{L}\bar{\boldsymbol{\lambda}} + \mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c) + \zeta\Delta\bar{\mathbf{u}}\end{aligned} \tag{5.3}$$

The individual weighed values are added, $\mathbf{w}^{-1} = 2\boldsymbol{\alpha}$, and the final voltage control while the system is under attack is then expressed as below.

$$\begin{aligned}\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\zeta\mathbf{w}^{-1}K_p\mathcal{L}\bar{\boldsymbol{\lambda}} + \mathbf{1}^\top\mathbf{w}\zeta\mathbf{w}^{-1}\mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c + \mathbf{1}^\top\mathbf{w}\zeta\Delta\bar{\mathbf{u}} \\ &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} + \mathbf{1}^\top\mathbf{w}\zeta\Delta\bar{\mathbf{u}}\end{aligned} \tag{5.4}$$

$\zeta$ is the new added weightings of the controller, and as $\zeta = \frac{1}{\mu}$ it is shown that with high enough control parameter $\mu$ the influence of the attack $\Delta\bar{\mathbf{u}}$ is reduced to the point where the average voltage regulation is achieved at the new equilibrium point of the system.

Control objective *1* is proven satisfied at the equilibrium while the system where subject to cyber attacks. However, with the modification of the controller, the consensus is again assessed in order to conclude that the modification does not prevent the controller in establishing consensus. Even though adding a scalar gain in front of the secondary controller, is assumed not to affect the ability to achieve consensus, this is addressed in order to define the most general conclusion. It is also interesting to see how the tuning of the two control parameters will affect the control system's ability to comply with the control objectives in steady state.

As the secondary control parameter $\zeta$ is added in front of the secondary controller, $\zeta$ will appear in associated dynamics due to the linearity of the system as given in 2.8. The final interconnected MG will therefore have $\zeta$ appearing in the cyber controller as $\mathbf{g}_c = -\zeta\mathcal{L}$. The equilibrium of the control network is therefore defined as:

$$\sum_c : \begin{cases}\dot{\mathbf{x}}_c = \mathbf{g}_c\mathbf{u}_c = -\zeta\mathcal{L}\mathbf{u}_c = -\zeta\mathcal{L}\boldsymbol{\lambda} & \mathbf{g}_c = -\zeta\mathcal{L} \\ \mathbf{y}_c = \mathbf{g}_c^\top\boldsymbol{\nabla}H_c(x_c) = -\zeta\mathcal{L}\boldsymbol{\nabla}H_c(x_c) = -\zeta\mathcal{L}\mathbf{K}^I\mathbf{x}_c\end{cases} \tag{5.5}$$

At steady state this control system is defined as:

$$0 = -\zeta\mathcal{L}\bar{\boldsymbol{\lambda}} \rightarrow -\zeta\mathcal{L}(2\boldsymbol{\alpha}\bar{\mathbf{I}}^{\mathcal{G}} + \boldsymbol{\beta}) = 0 \tag{5.6}$$

From the above system representation one can conclude that the network still is able to ensure consensus at the equilibrium for one equal incremental cost value. The adding of $\zeta = \frac{1}{\mu}$ will not prevent the system to cooperatively define the consensus as it is appearing before the Laplacian, and will only operate as a constant gain. This is also previously proven valid for the tuning of $\boldsymbol{\alpha}$. However, it is shown that if the control parameters are tuned so that $\mu \gg 2\boldsymbol{\alpha}$: i.e., $\zeta \ll 2\boldsymbol{\alpha}$ then the secondary controller is not able to ensure consensus at steady state. This is recognized as the time derivative of the system will tend to zero regardless of the consensus value, due to the significant small $\zeta$. In order to conclude that the second proposed resilient controller in *Hypothesis* 2 is sufficient in bringing the system to operate as uncompromised while being under attack in the control actuators, the *Assumption* 4 needs to hold.

**Assumption: 4.** *While $\mu$ is tuned to a significant high value above a given threshold, $\boldsymbol{\alpha}$ needs to be tuned with at least half the value of $\mu$.*

This assumption will also prevent turning off the secondary controller so that the system is only controlled by primary droop. If the modified controller defined in *Definition* 2 is tuned with only high $\mu$ then the secondary controller is turned off and the system is only able to ensure steady state operations at an equilibrium point, not ensuring the desired equilibrium. Hence, neither equal incremental costs nor weighted average voltage regulations are guaranteed at steady state operations.

It is then concluded that the modified controller combined with the proposed resilient control strategy ensures both control objectives at the systems new steady state equilibrium when $2\boldsymbol{\alpha} \geq \mu$. The effect of the potential cyber attacks in the control actuators is then reduced and *Hypothesis* 2 with *Assumption* 4 ensures to disregard the negative effects of only tuning the new secondary control parameter to a high value.

## 5.1 Simulations of Modified Control System

The cyber-physical MG is now simulated with the modified control system. The untuned parameter values, inherent event changes and cyber attack vectors are equally simulated as in *Part B* 5.6. However, the system

is now tested with tuning of $\boldsymbol{\alpha}$ and tuning of $\zeta$ in regards to the modified resilient controller. The base case scenario, with modified controller, is simulated in *Appendix* C where Figure C.2 and C.3 presents the system response of the unforced MG. The figures displays the same response as when the perturbed system was simulated for the firstly proposed PI-controller. This is due to fact that the the secondary control parameter firstly is untuned: i.e., $\zeta = \frac{1}{\mu} = \frac{1}{1}$. The modified controller is therefore proven correctly implemented, and the cyber attack in the control actuators is then implemented. Figure 5.2 and 5.3 shows the system responses of the system with modified controller and cyber attacks in the control actuators – without tuning the control parameters. The two figures features the same system responses of the perturbed system as presented in *Part B* Section 5.6. Hence, the implementation cyber attacks are correct, validating the subsequent conclusions of the new resilience property.

Figure 5.1: Perturbed MG under CA1 with Control Modifications

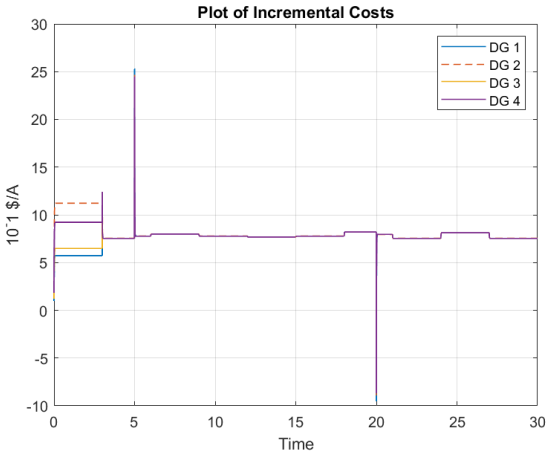


Figure 5.2: Incremental costs of perturbed system with modified controller

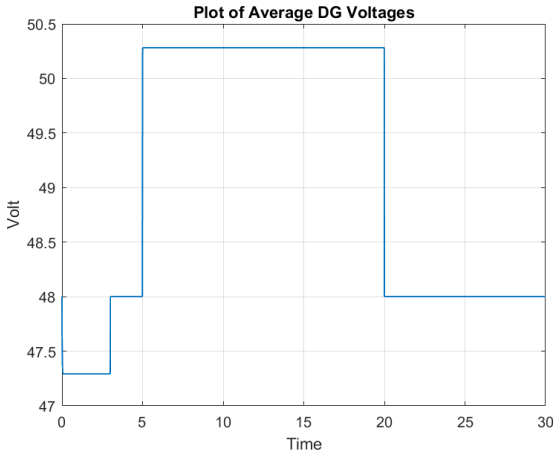


Figure 5.3: Average voltage of perturbed system with modified controller

The MG's performance with respect to equal incremental costs and average voltage regulation is respectively presented in 5.5 and 5.6. $\boldsymbol{\alpha}$ is tuned to the minimum resilience value 3000 and $\mu$ is tuned to the same value. This is a valid tuning strategy as $\boldsymbol{\alpha}$ is always multiplied with 2 in the implementations: i.e., $2\boldsymbol{\alpha} \geq \mu \rightarrow 2 \cdot 3000 \geq 3000$. The primary resilient control parameter will then have the double value of the second resilient control parameter satisfying the *Assumption* 4. In *Appendix* B the system exposed to cyber attacks in the control actuators are simulated for several tuning values of *only* the secondary control parameter $\mu$. Even tough it is previously proven that the tuning of $\boldsymbol{\alpha}$ did not improve the performance of the perturbed system, the simulations shows that tuning of only $\mu$ damages the ability to achieve consensus. However, the minimum necessary tuning of $\mu$ is assessed with respect to the average voltage regulation and proven sufficient when tuned to 3000.

Figure 5.4: Perturbed MG under CA1 with Control Modifications

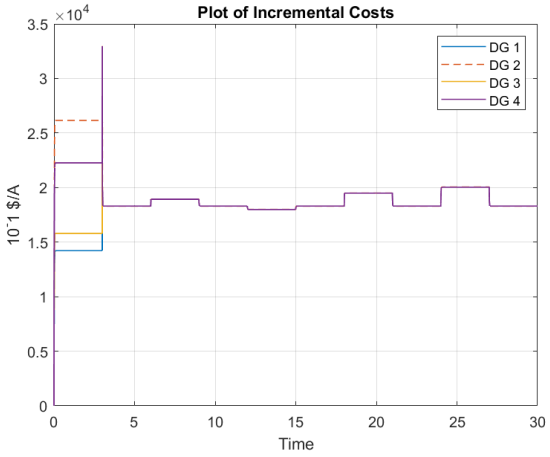


Figure 5.5: Incremental costs of perturbed system with both control parameters tuned to 3000

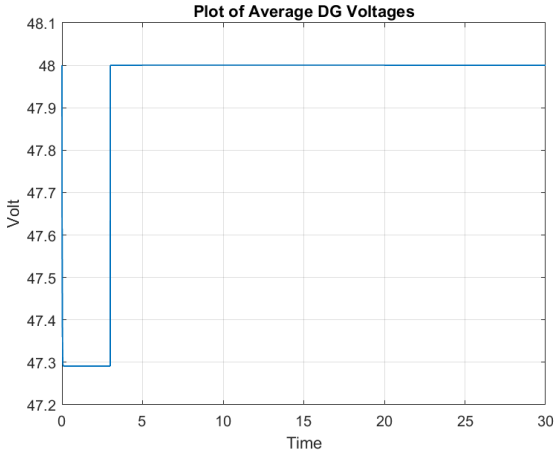


Figure 5.6: Average voltage of perturbed system with both control parameters tuned to 3000

From the above simulations it it shown that when the new resilient control strategy is implement, both the ability to ensure consensus and average voltage regulation is of higher performance. This it due to the fact that the attack is only perturbing in the actuators of the secondary controller i.e not disturbing in the interconnections between the physical network to the cyber network, and when $\zeta$ is multiplied and tuned in front on the secondary controller, the whole attack is cancelled out and will therefore not additionally disturb the consensus operations. Even though the system always was proven to satisfy the first control objective while being under attack, the above simulations shows that the performs of the cyber controller is optimized only for the scenario where both $\boldsymbol{\alpha}$ and $\mu$ are tuned to significant high values.

**Time Varying Cyber Attacks**

The modified controller is designed by studying the perturbed system prone to cyber attacks in the control actuators as this was the perturbed system mostly in need of a new resilient controller. The performance of the control modifications needs to be validated for both constant and time varying cyber attacks as mathematically conducted. The modified control performance is therefore tested by addressing the time varying cyber attack implemented as $\boldsymbol{\Delta u}(t) = [5 \cdot sin(t), 1, 0, 10]^\top$

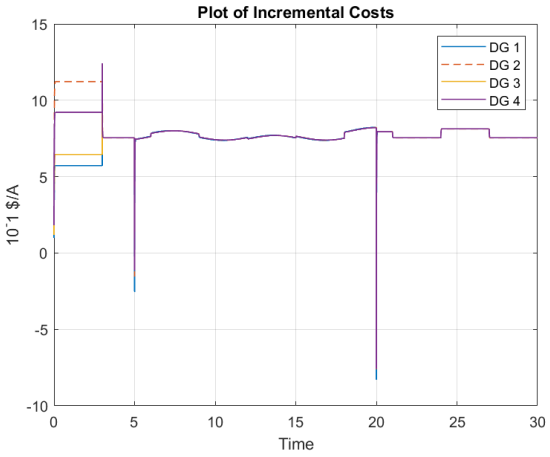


Figure 5.7: Incremental costs of time varying perturbed system, without resilience

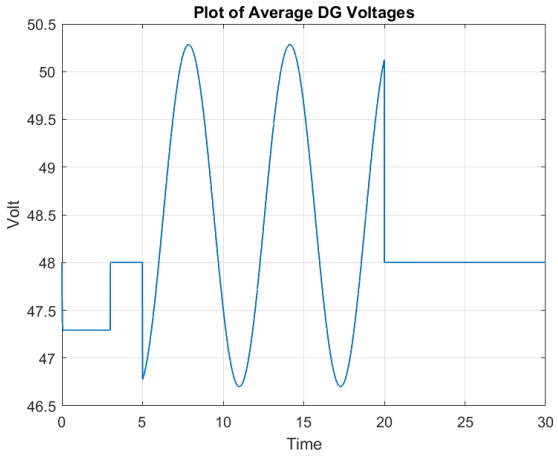


Figure 5.8: Average voltage of time varying perturbed system, without resilience

The figures above presents that both the incremental costs and the average voltage regulations are disturbed by the continuous and time varying cyber attack. However, Figure 5.7 certifies the above conclusions drawn – simulating the constant attack: i.e., the DGs are able to achieve consensus upon a value of the incremental costs of generation approximately equal to the equal incremental cost value of the unforced system: i.e., satisfying

control objective *1*. The average voltage regulation, presented in Figure 5.8 and Figure 5.3, shows that the voltage control is not ensured while the attack is intruding in the control actuators regardless of the attack is time varying or constant.

The same time varying cyber attack $\Delta\mathbf{u}(t)$ is now simulated with the tuned $\boldsymbol{\alpha}$ and $\mu$ equal to 3000. Figure 5.9 presents the same system response as Figure 5.5 and the controller is proven sufficient in operating the MG as approximately unforced with respect to the consensus property. The average voltage response in Figure 5.10 showcases that the second control objective is satisfied with appropriate tuning of the control parameters. The controller is therefore additionally concluded sufficient and robust against both the continuous and time varying attacks.

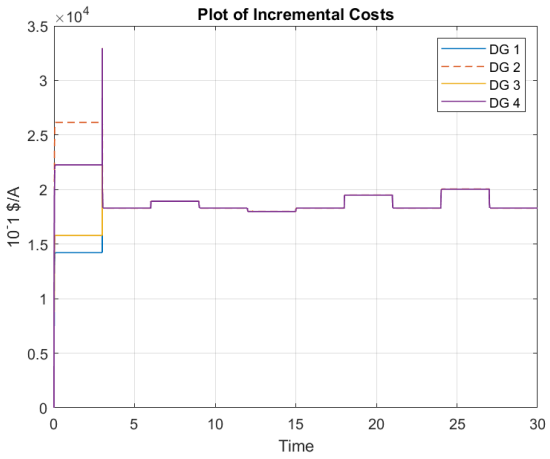


Figure 5.9: Incremental costs of time varying perturbed system with both control parameters tuned to 3000

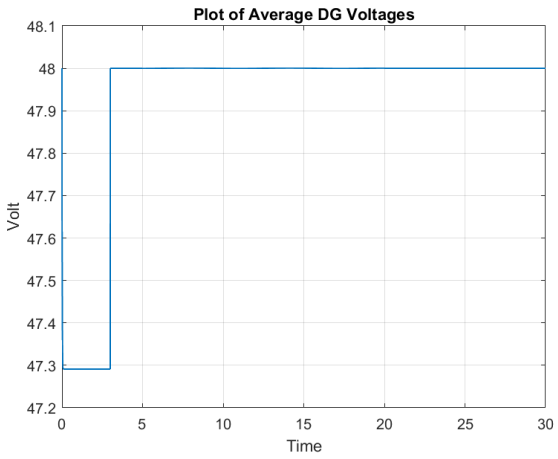


Figure 5.10: Average voltage of time varying perturbed system with both control parameters tuned to 3000

# 6 Cyber Attack 2: Equilibrium Analysis

In the previous equilibrium analysis of the system prone to cyber attacks in the current sensors, it was concluded that the proposed controller ensured control objective *2* and was able to ensure consensus. However, the consensus value was not equal to the optimal value: i.e., the control objective *1* was not satisfied. As seen in the conclusion of the first analysis, this type of attack was defined as a stealth attack and is even harder to identify and mitigate due to the fact that the control objectives often satisfied while the system is under attack. The objective of the new resilient control strategy is therefore to fist and foremost ensure that the modification at least does not change the ability to obtain consensus and average voltage regulation at the new equilibrium. The second desired conclusion is that the modified controller actually brings the system to a steady state equilibrium closer to the unforced systems equilibrium: i.e., ensuring that the consensus equals the optimal equal incremental cost values.

The modified closed loop control system with the potential attack in the current sensors is presented below.

$$\begin{aligned}\bar{\mathbf{u}}_{tot} &= \frac{1}{\zeta}\mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}(2\boldsymbol{\alpha}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta}) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \\ &= \frac{1}{\zeta}\mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P 2\boldsymbol{\alpha}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \qquad (6.1)\\ \bar{\mathbf{u}}_c &= 2\boldsymbol{\alpha}\bar{\mathbf{y}}_{tot}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta} \qquad (6.2)\end{aligned}$$

The primary control objective is then assessed at the equilibrium of the distributed control network, remembering to include the new dynamics where $\mathbf{g}_c = -\zeta\mathcal{L}$.

$$\sum_c : \begin{cases} 0 = \mathbf{g}_c\bar{\mathbf{u}}_c \\ \bar{\mathbf{y}}_c = \mathbf{g}_c^\top \boldsymbol{\nabla} H_c(\bar{\mathbf{x}}_c) \end{cases} \longrightarrow \begin{cases} 0 = -\zeta\mathcal{L}(2\boldsymbol{\alpha}(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) + \boldsymbol{\beta}) \\ \bar{\mathbf{y}}_c = -\zeta\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \end{cases} \longrightarrow \begin{cases} 0 = -\zeta\mathcal{L}\bar{\boldsymbol{\lambda}}^* \\ \bar{\mathbf{y}}_c = -\zeta\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c \end{cases} \qquad (6.3)$$

The above steady state distributed control network shows that the additional control parameter will not affect the influence of the attack. The same conclusion as for the cyber attack in the control actuators are drawn for

this case,: i.e., that the $\boldsymbol{\alpha}$ needs to be of equal or higher value that the $\zeta$ in order to ensure consensus. Hence, *Assumption* 4 needs hold in order to ensure robustness against the attack in the current sensors. However, when $2\boldsymbol{\alpha} \geq \frac{1}{\mu} = \zeta$ then the influence of the tuned new control parameter is removed both in front of the actual currents and the attack. It is therefore valid to conclude that the new resilient controller defined in *Definition* 2 combined with *Hypothesis* 2 with associated *Assumption* 4 will not affect the ability to ensure consensus, but it will not improve the desired mitigation of the attack. The cooperatively conducted incremental costs are still of higher values while the system is under attack.

Control objective *2* is then assessed at the new equilibrium with the desired result of not disturbing the system ability to ensure average voltage regulation even with the modified controller. When implementing the secondary controller defined in 6.1 and adding the individual weightings, the voltage control of the physical network is given as:

$$\begin{aligned}\mathbf{1}^\top \mathbf{w}\bar{\mathbf{V}} &= \mathbf{1}^\top \mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top \mathbf{w}\mathbf{R}^D(\bar{\mathbf{I}} + \Delta\bar{\mathbf{I}}) + \mathbf{1}^\top \mathbf{w}\zeta\left[\frac{1}{\zeta}\mathbf{R}^D(\bar{\mathbf{I}}^{\mathcal{G}} + \Delta\bar{\mathbf{I}}) - K_P\mathbf{w}^{-1}\mathcal{L}(\bar{\boldsymbol{\lambda}}^*) + \mathbf{w}^{-1}\mathcal{L}\mathbf{K}_I\bar{\mathbf{x}}_c\right] \\ &= \mathbf{1}^\top \mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top \mathbf{w}\zeta K_p\mathbf{w}^{-1}\mathcal{L}\bar{\boldsymbol{\lambda}}^* + \mathbf{1}^\top \mathbf{w}\zeta\mathbf{w}^{-1}\mathcal{L}\mathbf{K}^I\bar{\mathbf{x}}_c \\ &= \mathbf{1}^\top \mathbf{w}\mathbf{1}V_{nom} \end{aligned} \tag{6.4}$$

We arrive at the last equality accordingly, $\zeta$ and $K_P$ are implemented as constants and the Laplacian property $\mathbf{1}^\top\mathcal{L} = 0$ is then substantial in bringing the last terms to zero and the controller achieves average voltage regulation.

The equilibrium analysis concludes that the modified controller will not change the controller's ability to achieve consensus or the control objective *2*. However, it is also shown that the *Hypothesis* 2 does not improve the controller's ability to converge the system to an operating point closer to the equilibrium of the unforced system. Control objective *1* is therefore not satisfied at the new converged equilibrium while the system is under attack.

## 6.1 Simulations of Modified Control System

The performance of the modified controller is now tested for the perturbed system exposed to cyber attacks in the current sensors. The untuned parameter values, inherent event changes and cyber attack vectors are simulated as in *Part B* Section 6.5. However, the system is now tested with tuning of $\boldsymbol{\alpha}$ and tuning of $\zeta$ in regards to the modified resilient controller. The new simulated system is validated with the implemented modified controller and cyber attacks in *Appendix* C. The resilient modified controller is evaluated when both $\boldsymbol{\alpha}$ and $\zeta = \frac{1}{\mu}$ are tuned to the high resilient values, both defined equal to 3000 in *Appendix* B.

The simulations below validate the conclusions drawn in the above equilibrium analysis with respect to the two control objectives. In Figure 6.2 and 6.3 both of the control parameters are tuned to the minimum value of 3000 with the goal of ensuring resilience against the cyber attacks. $\boldsymbol{\alpha}$ is always multiplied with 2 in the dynamics and the primary control parameter will have the double value of the secondary control parameter, satisfying *Assumption* 4. The Figures validates the second conclusion stating that neither the tuning of $\boldsymbol{\alpha}$ nor the tuning or $\mu$ will ensure optimal operations defined when the achieved consensus values are equal to the unforced consensus values for each of the simulated the inherent events.

Figure 6.1: Perturbed MG under CA2 with Control Modifications

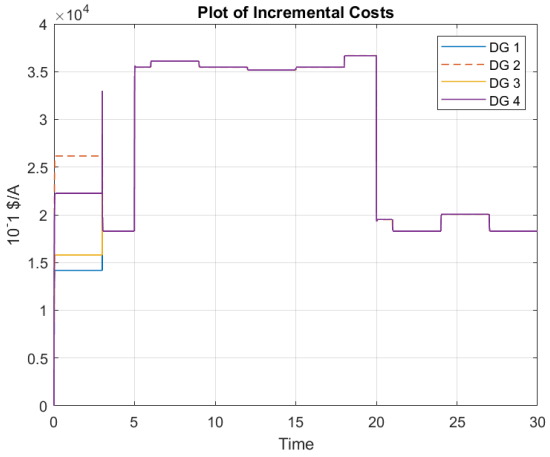


Figure 6.2: Incremental costs of perturbed system with both control parameters tuned to 3000

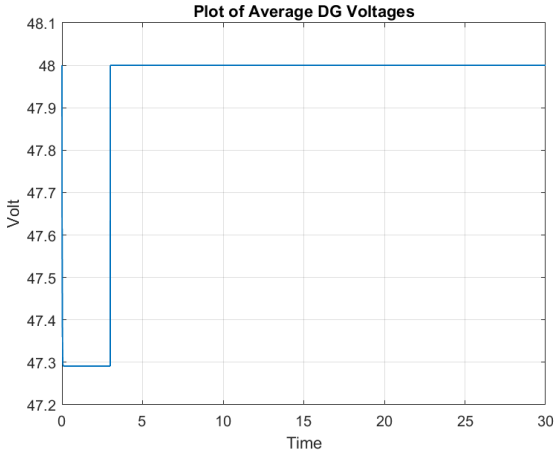


Figure 6.3: Average voltage of perturbed system with both control parameters tuned to 3000

The simulations in this section combined with the simulations of the perturbed system, subject to the second cyber attack, with the first proposed resilient controller displays that the modified controller may have very high $\boldsymbol{\alpha}$ without perturbing the controller's ability to ensure the two control objectives at the equilibrium. However, Figure 6.4 displays the negative effect of high $\mu$ without tuning $\boldsymbol{\alpha}$ to either the same value or a higher value.

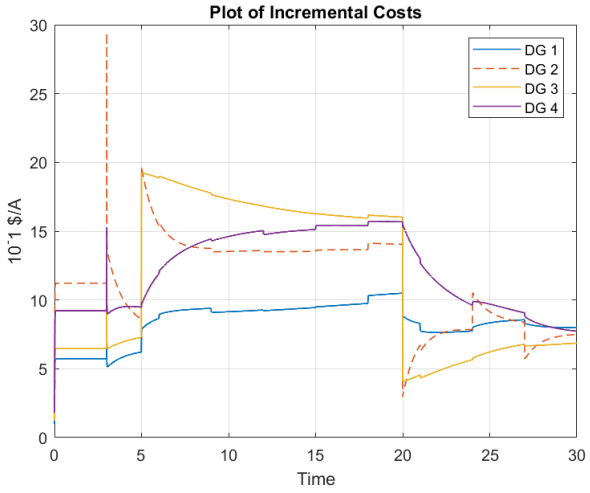


Figure 6.4: Incremental cost when only $\mu = 3000$

The system is therefore proven able to operate at an steady state equilibrium where consensus is achieved and the control objective *2* is ensured for the three defined control scenarios: (1) when the controller are of regular control parameter values: i.e., untuned; (2) when only $\boldsymbol{\alpha}$ is of significant high value; (3) when both $\boldsymbol{\alpha}$ and $\zeta$ are tuned to significant high values.

# 7 Cyber Attack 3: Equilibrium Analysis

The equilibrium analysis performed before the control modification, concluded that the resilient controller from *Hypothesis* 1 was sufficient in removing the influence of the attack. The sufficient tuning of $\boldsymbol{\alpha}$ ensured that the system was able to operate as unforced with respect to the first control objective. Control objective *2* was satisfied regardless of the presence of these attacks in the communication links and regardless of the tuning of $\boldsymbol{\alpha}$.

The stability analysis in *Part C* Section 3 presented that the perturbed system still always is ISS regardless of the attacks. This new equilibrium analysis is then conducted with the ambition of concluding that the modified controller does not disturb the controller's ability to ensure the two control objectives at the new equilibrium. First, the closed loop control system with the modified controller needs to be establish. The functions of the two controllers are obtained by implementing the attack vectors equally as done in *Part B* Section 6.2. However, the attacks are now added to the closed loop defined in 2.6 in *Part C* with the modified controller. The controllers at the equilibrium of the perturbed system are then defined below.

$$\begin{aligned}\bar{\mathbf{u}}_{tot} &= \frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\boldsymbol{\alpha}(K_p\bar{\mathbf{z}}^{*\lambda} - \bar{\mathbf{z}}^{*c}) \\ &= \frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + 2\alpha(-K_p\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}^I(\bar{\mathbf{x}}^c + \Delta\bar{\mathbf{x}}^c)) \qquad (7.1)\\ \bar{\mathbf{u}}_c &= 2\boldsymbol{\alpha}\bar{\mathbf{I}}^{\mathcal{G}} + \boldsymbol{\beta} = \boldsymbol{\lambda} \qquad (7.2)\end{aligned}$$

The primary control objective is firstly assessed by studying the distributed control network with the modified controller:

$$\sum_c : \begin{cases}\dot{\mathbf{x}}_c = \mathbf{g}_c\mathbf{u}_c = -\zeta\mathcal{L}(\mathbf{u}_c + \Delta\boldsymbol{\lambda}) = -\zeta\mathcal{L}(\boldsymbol{\lambda} + \Delta\boldsymbol{\lambda}) & \mathbf{g}_c = -\zeta\mathcal{L} \\ \mathbf{y}_c = \mathbf{g}_c^\top\boldsymbol{\nabla}H_c(x_c + \Delta\mathbf{x}_c) = -\zeta\mathcal{L}\boldsymbol{\nabla}H_c(x_c + \Delta\mathbf{x}_c) = -\zeta\mathcal{L}\mathbf{K}^I(x_c + \Delta\mathbf{x}_c)\end{cases} \qquad (7.3)$$

The steady state equilibrium of the distributed control network is proven to achieve consensus when:

$$0 = -\zeta\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) \rightarrow -\zeta\mathcal{L}((2\boldsymbol{\alpha}\bar{\mathbf{I}}^{\mathcal{G}} + \boldsymbol{\beta}) + \Delta\bar{\boldsymbol{\lambda}}) = 0 \qquad (7.4)$$

It is shown that both the cooperative optimal incremental cost value and the cooperative defined attack value will be cancelled out by increasing $\mu = \zeta^{-1}$ to a significant high value. For the attack in the communication links, it is important to counteract the effect of bringing the cyber states to zero without needing to obtain one consensus value. With both high $\boldsymbol{\alpha}$ and high $\mu$ the control network will achieve an equilibrium point only when the consensus value for the incremental costs is defined: i.e., disregarding the attack $\Delta\bar{\boldsymbol{\lambda}}$. This will always be valid when $2\boldsymbol{\alpha} \geq \zeta = \frac{1}{\mu}$ and *Assumption* 4 is therefore proven valid and necessary when the tuning of the control parameters is performed in order to reduce the influence of the attacks.

Control objective *2* is then assessed with the proposed modifications. Voltage regulation at the equilibrium point of the electrical system, with the new control system, is expressed as $\bar{\mathbf{V}} = \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \zeta\bar{\mathbf{u}}_{tot}$. By implementing the cyber attacks, the final voltage regulation is given by:

$$\begin{aligned}\bar{\mathbf{V}} &= \mathbf{1}V_{nom} - \mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} + \zeta\left[\frac{1}{\zeta}\mathbf{R}^D\bar{\mathbf{I}}^{\mathcal{G}} - 2\boldsymbol{\alpha}K_p\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) + 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}^I(\bar{\mathbf{x}}_c + \Delta\bar{\mathbf{x}}^c)\right] \\ &= \mathbf{1}V_{nom} - \zeta 2\boldsymbol{\alpha}K_p\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) + \zeta 2\boldsymbol{\alpha}\mathcal{L}\mathbf{K}^I(\bar{\mathbf{x}}_c + \Delta\bar{\mathbf{x}}^c) \qquad (7.5)\end{aligned}$$

The individual weighed values are implemented, and by expressing $\mathbf{w}^{-1} = 2\boldsymbol{\alpha}$ the final average voltage regulation, while the system is under attack, is then expressed as:

$$\begin{aligned}\mathbf{1}^\top\mathbf{w}\bar{\mathbf{V}} &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} - \mathbf{1}^\top\mathbf{w}\zeta\mathbf{w}^{-1}K_p\mathcal{L}(\bar{\boldsymbol{\lambda}} + \Delta\bar{\boldsymbol{\lambda}}) + \mathbf{1}^\top\mathbf{w}\zeta\mathbf{w}^{-1}\mathcal{L}\mathbf{K}^I(\bar{\mathbf{x}}_c + \Delta\bar{\mathbf{x}}^c)) \\ &= \mathbf{1}^\top\mathbf{w}\mathbf{1}V_{nom} \qquad (7.6)\end{aligned}$$

We arrive at the last equality accordingly, $\zeta$ and $K_P$ are implemented as constants and the Laplacian property $\mathbf{1}^\top\mathcal{L} = 0$ is then instrumental in bringing the last terms to zero and the controller achieves average voltage regulations.

The equilibrium analysis concludes that the modified controller from *Definition* 2 combined with *Hypothesis* 2 will not change the controller's ability to satisfy the two control objectives, with appropriate tuning given in *Assumption* 4. The modifications will therefore ensure that the MG operates under desired conditions, equally ensured by the proposed resilient controller in *Hypothesis* 1.

## 7.1 Simulations of Modified Control System

When the robustness against cyber attacks in the communication links were previously simulated in *Part B* Section 7.5, both the untuned PI-controller and the resilient strategy presented in *Hypothesis* 1 were addressed. It was then proven both mathematically and validated by simulations, that the perturbed system needed the

minimum tuning of $\boldsymbol{\alpha}$ in order to establish a consensus value corresponding to the optimal value of the incremental costs of generation.

This section aims to simulate and conclude that the new modified controller, with appropriate values of $\mu$ and $\boldsymbol{\alpha}$, will not disturb the performance of the first proposed resilient controller. In this section the untuned parameter values, inherent event changes and cyber attack vectors are equally simulated as in *Part B* Section 7.5, now combined with the control modifications. The new simulated system is validated with the implemented modified controller and cyber attacks in *Appendix* C. The resilient modified controller is assessed in this section where both $\boldsymbol{\alpha}$ and $\mu$ is tuned to the significant resilient values defined in *Appendix* B and B.

Figure 7.2 and 7.3 presents the system response of the modified control system with both $\boldsymbol{\alpha}$ and $\mu$ equal to 3000, previously defined to satisfy *Hypothesis* 2 and *Assumption* 4. The simulations displays that the modified controller brings the system to operate identically as the simulated system response when only $\boldsymbol{\alpha}$ were tuned to high values. It is therefore proven that the system is operating as close to the unforced equilibrium as possible for the two defined control scenarios: (1) when only $\boldsymbol{\alpha}$ is tuned to significant high value; (2) when both of the two control parameter are tuned to significant high values.

Figure 7.1: Perturbed MG under CA3 with Control Modifications

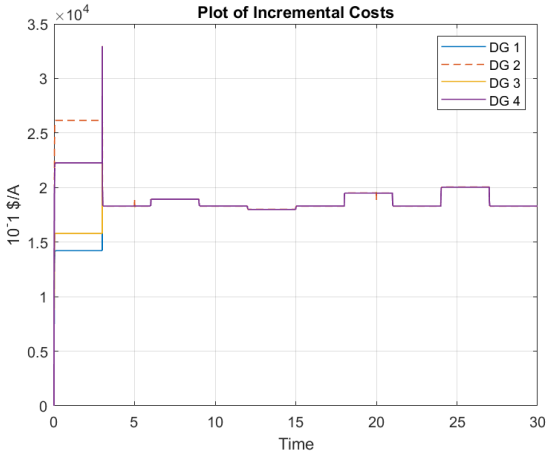


Figure 7.2: Incremental costs of perturbed system with both control parameters tuned to 3000

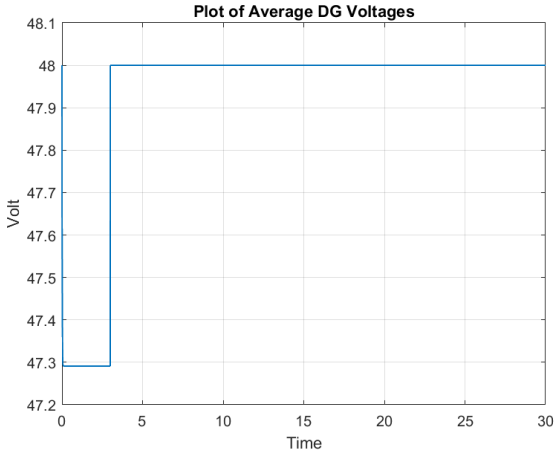


Figure 7.3: Average voltage of perturbed system with both control parameters tuned to 3000

## Part D:

# Conclusion

This thesis presented the modelling of the cyber-physical DC microgrid in closed loop with a resilient secondary controller ensuring optimal steady state operation. More precisely, the individual DGs forming the microgrid network are equipped with local primary droop control limiting the voltage deviations from the nominal voltage. Although useful to stabilize the system and limit deviations, the primary controller is not sufficient to ensure that the pre-defined optimal control objectives for the overall interconnected CP MG are met, due to the decentralized nature of the droop. Therefore, an additional outer loop distributed controller is introduced as a secondary controller for the MG. The secondary controller uses communication between the neighbouring units in order to establish an agreement between the DGs, as its design is based on the consensus protocol. The cyber-physical MG is then modelled based on energy principles and the closed loop control ensures convergence to a steady state at the equilibrium where the two pre-defined control objectives are satisfied.

Due to the use of communication links in the distributed control network, the cyber-physical MG is prone to cyber attacks and the control system needs to be tuned and modified in order to ensure robustness against the potential cyber threats. The perturbed system is assessed with respect to three different cyber attacks and the resilience property is tested and modified in order to improve its robustness. All the final conclusions presented in this thesis are theoretically obtained and further validated with simulations. They are also validated both for constant and continuous time varying cyber attacks.

# 1 Resilient Control Strategy Ensuring Robustness against Cyber Attacks

When the system is assessed as a power system subject to cyber threats, the cyber-physical MG is modelled as a perturbed system with external continuous and time varying inputs. The microgrid in closed loop with the proposed control is ISS, which guarantees bounded stable states when potential bounded attacks intrude. Therefore, the perturbed system always converges to a new equilibrium – close to the desired equilibrium – within a bounded limit enforced by the bounded attack. The proposed resilient control strategies are then assessed at this new equilibrium, evaluating if the controller is able to bring the system to the desired operations where the two control objectives are satisfied, while being under attack.

The first resilient strategy, proposed in *Hypothesis* 1 does not affect the first or second types of cyber attacks under consideration; i.e., cyber attacks in the control actuators and in the current sensors. Hence, the tuning of the primary control parameter $\boldsymbol{\alpha}$ will not support mitigating the influence of those attacks. However, it is also observed that this tuning does not disturbs the ability to potentially ensure the control objectives. When the third MITM cyber attack – intruding in the communication links – is considered, the proposed resilient strategy is concluded to efficiently remove the influence of the attacks. The sufficient tuning of $\boldsymbol{\alpha}$ is established equal to 3000 in the *Appendix* B, and it is proven that tuning the primary control parameter to the defined threshold value ensures that the system either operates as unchanged or as unforced.

The controller is then modified aiming to mitigate the disadvantages caused by the two first cyber attacks. It is concluded that the new resilient strategy proposed in *Hypothesis* 2 improves the resilience when *Assumption* 4 holds for the modified controller given in *Definition* 2. The modified controller includes adding a new secondary control parameter $\zeta = \frac{1}{\mu}$ and the sufficient tuning of $\mu$ is defined in the *Appendix* B equal to 3000. The resilient strategy is concluded to improve the robustness when cyber attacks adds false data to the actuators of the controller as it is able to ensure average voltage regulations due to the tuning of the secondary control parameter. It is also observed that optimizing control objective *2* consequently affects the consensus property and the proposed resilient control strategy ensures that the perturbed system operates as unforced at steady state while being under attack.

Even though the first resilient control strategy ensures robustness against MITM attacks in the communication links and the second control strategy ensures resilience against both MITM attacks in the communication links and against FDI attacks in the actuators of the controller, *the proposed controller is still not able to ensure robustness against stealth attacks intruding in the current sensors.* More precisely, the perturbed controller is able to ensure proper operations of the MG: i.e., ensuring average voltage regulations and cooperatively defining a consensus value. However, the consensus value does not correspond to the optimal consensus value equivalent with the equal incremental cost of generation. It is observed that the stealth attack is able to trick the system operator by not disturbing the operations of the MG, and the resilient strategy is not concluded sufficient in ensuring robustness against all cyber threats. This is due to more discrete intrusion of stealth attacks. The false data is added with respect to the same dynamics as the actual currents, and control parameters will therefore equally effect the measured currents and the false values. The controller uses control feedback in order to ensure proper operations of the MG and robustness against cyber attacks. When it is the main feedback value that is perturbed the proposed resilient strategies and modified controller will not be sufficient as their performance is highly dependent on the feedback. The second resilient strategy is therefore not able to reduce the influence of the FDI attack in the currents sensors and the system is not operating as unforced at the converged steady state equilibrium. Hence, the resilient controller needs to be further modified in order to ensure optimal robustness.

This thesis concludes that the modified controller – with sufficient resilient tuning – improves the robustness against cyber threats. The controller is capable of always ensuring average voltage regulation, with the appropriate tuning of the control parameters, and the cyber controller will always cooperatively obtain a consensus value. However, the consensus value is not confirmed to always satisfy the primary control objective: i.e., the equal incremental cost criteria. The controller needs to be further modified in order to resolve the resilience problem with respect to the stealth attacks and thereby satisfying the final control objective: *ensuring novel robustness against all potential cyber threats.*

# 2 Further work

As explained in the above section, the control dynamics and resilient control strategy needs to be further modified in order to completely robustify the control system. This is left for further studies combined with the transient performance analysis and potential design modifications of the CP MG. This thesis presents the linear model of the cyber-physical MG, associated stability analysis, and equilibrium assessment. Hence, it facilitates and act as a starting point of further topics as considered to be investigated.

Further control configuration assessments are deemed as the next step in the evaluation of CP MGs. When the proposed resilient strategies are implemented, multiple system states will subsequently be tuned and amplified. This might cause new disadvantages when considering other properties beyond stability and optimal control operations. When the attack disturbs the ability to achieve optimal consensus value it is shown that the tuning of the primary control parameter is sufficient in ensuring unforced optimal operations. However, this tuning will additionally cause high equal incremental costs. Even though the consensus value is achieved, it is amplified which may cause operational changes with respect to e.g. the generated currents or consumed power in the loads. This thesis also shows that the tuning of the primary control parameter scales the voltages of the DGs which is proven to not effect the stability or the ability to ensure the control objectives. However, the effect of the high voltages may disturb other preferable operations. Further control assessment could therefore include investigating the effects of potential high voltages and high consensus values, combined with the transient control performance and appropriate resilient tuning. The goal of the further analysis would then be to optimize the MGs with respect to stability, robustness, fast and ideal operations.

Further studies concerning the model of the CP DC MG are also of great importance in order to obtain one final generalized stability certificate. The modelled MG, presented in this thesis, only admits linear dynamics by disregarding any potential nonlinear characteristics such as the constant power loads or nonlinear converters. The obtained Lyapunov certificate may serve as a starting point if later applying nonlinear dynamics and aiming to obtain one final stability certificate valid for both linear and nonlinear systems. The used *Lemmas* defined in Khalil's Nonlinear control [23] are then no longer applicable as the nonlinear systems first need to be proven exponentially stable. This is not a generalized proof, as presented for the linear case, and the perturbed nonlinear systems need to be proven ISS for every intrusion of the bounded cyber attacks. Hence, the nonlinear dynamics lead to even more complex deductions of the ISS certificates. This causes difficulties when later conducting the equilibrium analysis assessing the influence of the cyber attacks. Additionally, presented theory in Khalil's Nonlinear control [23] may be used to obtain the bound of the attack, as presented in this thesis for the first studied bounded cyber attack. The obtained function of the bound may then be used to reduce the bound: i.e., giving a more restricted ISS solution space, however ensuring that the converged equilibrium is closer to the optimal equilibrium of the unforced system.

Voltage regulation may also be further optimized, aiming to ensure independent voltage containment by replacing control objective *2*. It is desirable that the weighted sum of all the voltages is equal to the pre-defined nominal voltage. However, the control objective *2* does not limit the deviations between the DG's voltages. By modifying the optimization algorithm, independent voltage containment might be ensured: i.e., limiting the individual voltage deviations with respect to the pre-defined nominal voltage. This will serve as a stronger second objective, further optimizing the operations of the MG.

# Bibliography


[1] B. Abdolmaleki and G. Bergna-Diaz. 'Distributed Control and Optimization of DC Microgrids: A Port-Hamiltonian Approach'. In: *IEEE* (Aug. 2021).

[2] D.M. Ferreira et al. 'Overview of Consensus Protocol and its Application to Microgrid Control'. In: (2015), pp. 1–16.

[3] A. Vasilakis et al. 'The Evolution of Research in Microgrids Control'. In: (2020).

[4] M. Jain et al. 'Real-Time Implementation of Islanded Microgrid for Remote Areas'. In: *Journal of Control Science and Engineering* (2016).

[5] Transmission and Distribution Committee. 'IEEE Standard for the Specification of Microgrid Controllers'. In: *IEEE Standards Association* (2017).

[6] M. Tucci et al. 'A decentralized scalable approach to voltage control of DC islanded microgrids'. In: *IEEE Transactions on Control Systems Technology* 24.6 (2016), pp. 1965–1979.

[7] M.S. Sadabadi, Q. Shafiee and A. Karimi. 'Plug-and-Play Robust Voltage Control of DC Microgrids'. In: *IEEE Transactions on Smart Grid* 9.6 (2018), pp. 6886–6896.

[8] M. Cucuzzella, S. Trip and J. Scherpen. 'A Consensus-Based Controller for DC Power Networks'. In: *Conferance Paper* (2015).

[9] A. van der Schaft and D. Jeltsema. 'Port-Hamiltonian Systems. Theory: An Introductory Overview'. In: *Foundations and Trends in Systems and Control* 1.2-3 (2014), pp. 173–378.

[10] R. Ortega et al. 'Control by Interconnection and Standard Passivity-Based Control of Port-Hamiltonian Systems'. In: *IEEE Transactions on Automatic Control* 53.11 (2008).

[11] S. Boyd and L. Vandenberghe. *Convex Optimization*. University Press, 2004.

[12] S.J. Wood, B.F. Wollenberg and G.B. Sheblé. *Power generation, operation and control*. 3rd ed. Wiley, 2014.

[13] S.Sahoo et al. 'Distributed Screening of Hijacking Attacks in DC Microgrids'. In: *IEEE Transactions on Power Electronics* 35.7 (2020), pp. 7574–7582.

[14] M.S. Sadabadi, S. Sahoo and F. Blaabjerg. 'Stability-Oriented Design of Cyberattack-Resilient Controllers for Cooperative DC Microgrids'. In: *IEEE Transactions on Power Electronics* 37.2 (2022), pp. 1310–1321.

[15] O.A. Beg, T.T. Johnson and A. Davoudi. 'Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids'. In: *IEEE Transactions on Industrial Informatics* 13.5 (2017), pp. 2693–2703.

[16] M.S. Sadabadi. 'Attack-Resilient Distributed Control in DC Microgrids'. In: *2021 European Control Conference (ECC)* (2021), pp. 503–508.

[17] D. Annavaram, S.Sahoo and S.Mishra. 'Stealth Attacks in Microgrids: Modeling Principles and Detection'. In: *2021 9th IEEE International Conference on Power Systems (ICPS)* (2021), pp. 1–6.

[18] S.Sahoo et al. 'On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach'. In: *IEEE Transactions on Industrial Electronics* 67.8 (2020), pp. 6562–6571.

[19] A.Cecilia et al. 'Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads'. In: *IEEE Transactions on Power Electronics* (2021).

[20] M.Mola et al. 'Distributed Event-Triggered Consensus-Based Control of DC Microgrids in Presence of DoS Cyber Attacks'. In: *IEEE Access* 9 (2021), pp. 54009–54021.

[21] S. Subham, T. Dragičević and F. Blaabjerg. 'Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids'. In: *IEEE Transactions on Power Electronics* 36.3 (2021), pp. 2522–2532.

[22] M.S. Sadabadi and A. Gusrialdi. 'On Resilient Design of Cooperative Systems in Presence of Cyber-Attacks'. In: *2021 European Control Conference (ECC)* (2021), pp. 946–951.

[23] H. K. Khalil. *Nonlinear Control*. 1 st. Pearson Education, 2015.

[24] J.G. Balchen, T. Andersen and B.A. Foss. *Reguleringsteknikk*. 6th ed. NTNU Grafisk Senter, 2016.

[25] H. K. Khalil. *Nonlinear systems*. 3rd ed. Pearson Education, 2014.

[26] B. Jayawardhana et al. 'Passivity of Nonlinear Incremental Systems: Application to PI Stabilization of Nonlinear RLC Circuits'. In: *IEEE Conference on Decision and Control* 18.3 (2006).

[27] A. Quarteroni, R. Sacco and F. Saleri. *Numerical Mathematics*. Springer-Verlag New York, Inc, 2000.

# Appendix

## A Choosing the Parameter Values

The simulations conducted to test the control performance of both the perturbed and unforced case specific MG, are all based on the same inherent dynamics. The parameters of the electrical network and the distributed control network are equally defined in all the simulations when disregarding the dynamics related to the external cyber attacks. The implemented parameters are obtained from both standard values, influenced by Babak's publication [1] and by multiple testings of the MG. The case specific MG is based on low voltage where 48 $[V]$ is chosen as the reference voltage level of the grid. The per unit, $[p.u]$, values of the loads and transmission lines in Table A.3 and Table A.2 are defined for the RL base value of $(50\Omega, 50\mu H)$. The three Tables below shows the inherent values of the DGs, transmission lines and loads and are parameter values implemented for all the simulations in this thesis.

Table A.1: Parameter Values of the DGs

| Parameters | DG number i $\in \mathcal{G}$ | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| $I_i^{rated}\ [A]$ | 15 | 6 | 12 | 12 |
| $\Delta V_{max}\ [V]$ | 3 | | | |
| $R_i^{\mathcal{D}}[V]/[A]$ | 0.2 | 0.5 | 0.25 | 0.25 |
| $R_i^{\mathcal{G}}[p.u]$ | 0.5 | 0.4 | 0.55 | 0.6 |
| $L_i^{\mathcal{G}}[p.u]$ | 0.5 | 0.4 | 0.55 | 0.6 |
| $U_i^{\mathcal{G}}$ | 0 | 0 | 0 | 0 |

Table A.2: Parameter Values of the Transmission Lines

| Parameters | TL number j $\in \mathcal{E}$ | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| $R_j^{\mathcal{E}}[p.u]$ | 1 | 2 | 2 | 1 | 1 |
| $L_j^{\mathcal{E}}[p.u]$ | 1 | 2 | 2 | 1 | 1 |

Table A.3: Parameter Values of the Loads

| Parameters | load number k $\in \mathcal{N}$ | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| $C_k^{\mathcal{N}}[F]$ | $22 \times 10^{-3}$ | | | |
| $1/G_k^{\mathcal{N}}[\Omega]$ | 30 | 20 | 20 | 20 |
| $I_k^{cte}[A]$ | 0.5 | 0.6 | 0.4 | 0.5 |

## B Additional Simulations Substituting Chosen Values

This section includes additional simulations used to defined the appropriate tuning values of the control parameters. The obtained values are used as the minimum significant tuning values sufficient in ensuring resilience while the MG is subject to cyber attacks.

### Minimum Resilience Value of Primary Control Parameter

In order to establish the sufficient tuning value of $\boldsymbol{\alpha}$, the system prone to cyber attacks in the communication links is tested with different resilience values. This perturbed system is mathematically proven to be the only system not able to ensure consensus while being under attack. The system analyses of this thesis also shows that the tuning of the primary control parameter only supports robustness against the disturbed consensus property and will not influence the desired average voltage regulations.

As the third assessed perturbed system is the only MG not able to satisfy the primary control objective: i.e., not achieving consensus, the minimum resilience value is obtained by testing the control performance for various values of $\boldsymbol{\alpha}$. The intention is then to establish the threshold for the minimum tuning value, sufficient in always ensuring that the primary control objective is satisfied if the consensus property is disturbed.

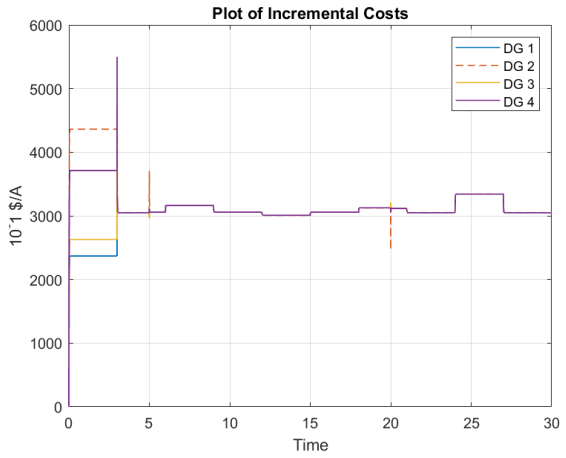


Figure B.1: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=500

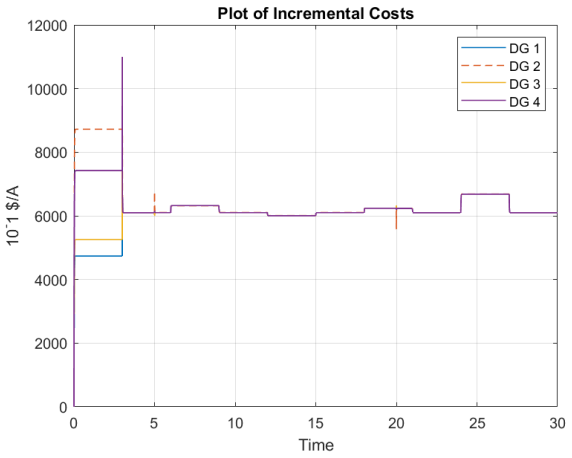


Figure B.2: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=1000

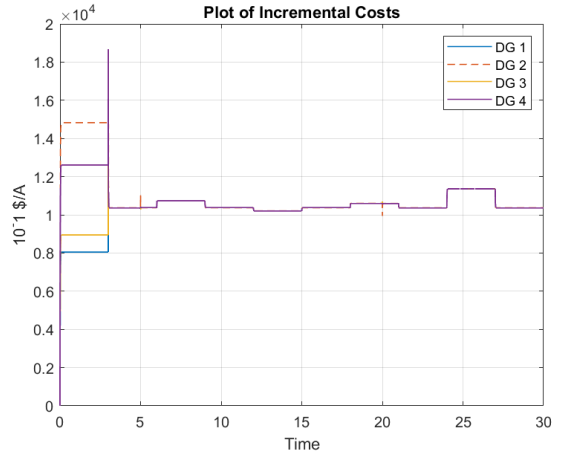


Figure B.3: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=1700

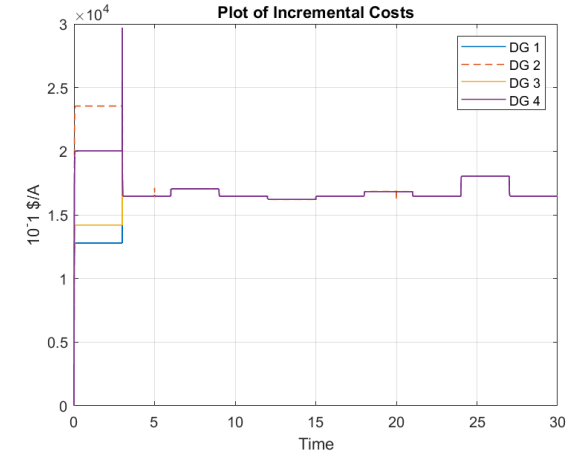


Figure B.4: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=2700

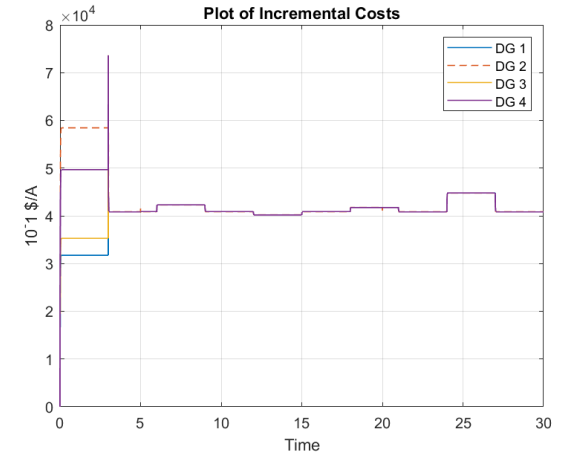


Figure B.5: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=6700

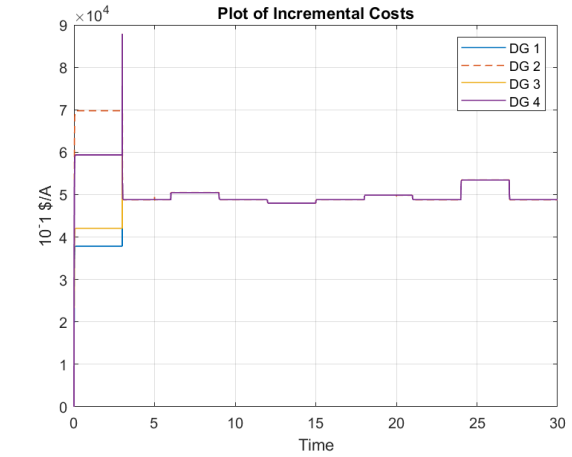


Figure B.6: Incremental costs of perturbed system with $\boldsymbol{\alpha}$=8000

The above figures shows that $\boldsymbol{\alpha}$ needs to have the values of 8000 to almost completely remove the disadvantage

caused by the attack. Due to Simulink it is not possible to run higher simulations than 8000. However, studying the figures above validates that 8000 is high enough to conclude that the system operates as unforced. It is also recognized that the value of alpha will have higher impact on the system when the parameter are of smaller tuning values. When $\boldsymbol{\alpha}$ is increased above a certain threshold the further tuning will impact the system to a less degree. It is therefore concluded that this threshold value defines the minimum and sufficient parameter value, necessary in bringing the system to operate as close to the unforced system as possible. The figures above shows that $\boldsymbol{\alpha} = 3000$ is an approximate threshold, further used as the minimum significant value of $\boldsymbol{\alpha}$ when the resilience is tested throughout the master.

## Minimum Resilience Value of Secondary Control Parameter

The studied perturbed systems of this thesis presents that the cyber attack introducing in the control actuators is the only attack disturbing the ability to ensure average voltage regulation. Hence, the first studied perturbed system where the only system requiring the control modifications and the significant tuning of $\mu$ is obtained by testing the resilience property of the control performance of this system. The desired result is to establish the minimum necessary value of $\mu$ sufficient in always ensuring that the average voltage regulation is satisfied regardless of the presence of a cyber attack.

Figure B.7: Resilience test when tuning only the secondary control parameter to 700

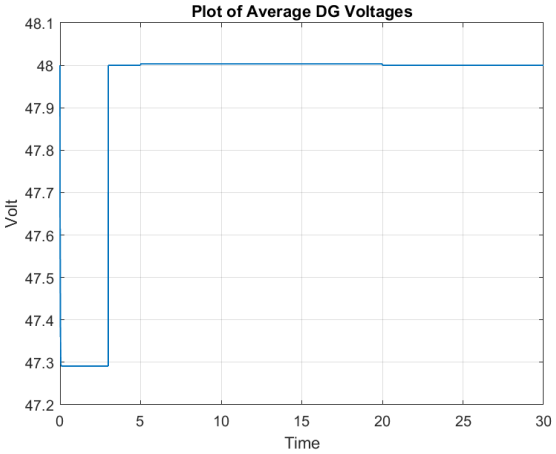


Figure B.8: Average voltage of perturbed system with modified controller

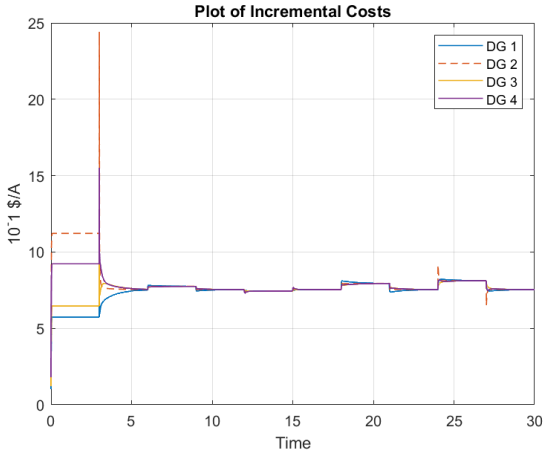


Figure B.9: Incremental costs of perturbed system with modified controller

Figure B.8 shows that the tuning of $\mu = 700$ is not sufficient in completely removing the attack. Additionally it is recognized that the tuning of only $\mu$ destroys the system's ability to achieve consensus upon the equal incremental costs of generation. The system is then tested for the potential resilience value $\mu = 1700$ and Figure B.11 shows that the average voltage regulation still is disturbed when the attack is intruding. Figure B.12 emphasizes this conclusion as the attack increases the voltage above $48V$ at the time step of 5 seconds: i.e., when the attack is intruding. However, it is recognized that higher tuning of $\mu$ brings the system to operate closer to the desired conditions even though Figure B.13 shows that the incremental costs are deviating even more from the unified consensus value.

Figure B.10: Resilience test when tuning only the secondary control parameter to 1700

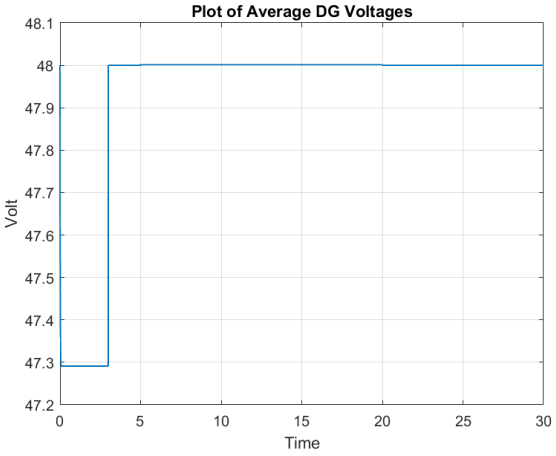


Figure B.11: Average voltage of perturbed system with modified controller

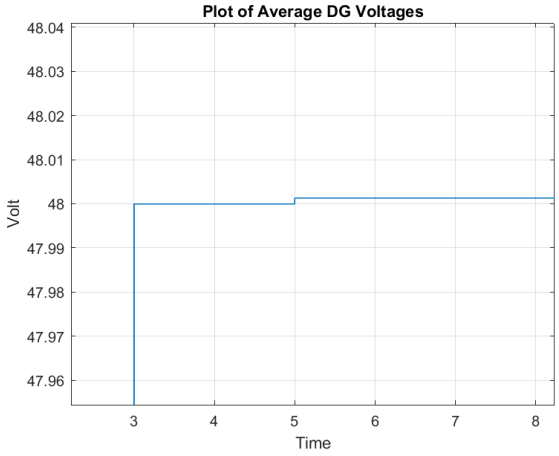


Figure B.12: Average voltage of perturbed system with modified controller

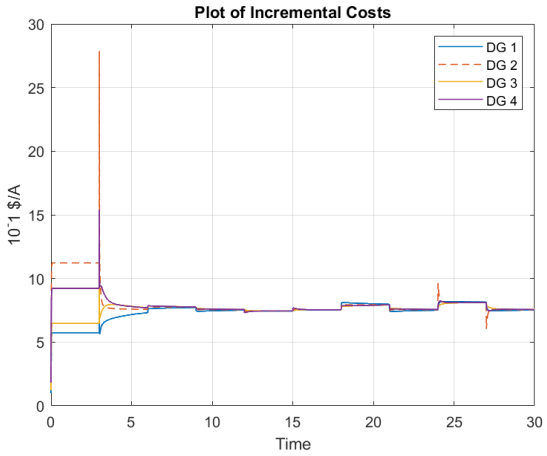


Figure B.13: Incremental costs of perturbed system with modified controller

Even though the above simulations show extreme small voltage deviation from the desired average of $48V$ the tuning is increased in order to see if it is possible to completely remove the effect of the attacks with respect to the voltage regulations. This effect might be of more severe importance when the resilience is tested on larger scale MG's or on medium/high voltage MG's. The control performance is then tested when the minimum resilience is equal to $\mu = 2500$ and $\mu = 2700$, $\mu = 3000$ respectively in Figure B.15, Figure B.16 and Figure B.17.

Figure B.14: Resilience test when tuning only the secondary control parameter higher values

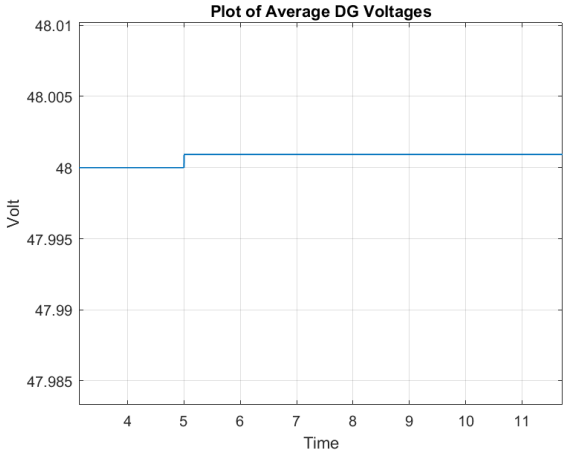


Figure B.15: Average voltage of perturbed system with $\mu = 2500$

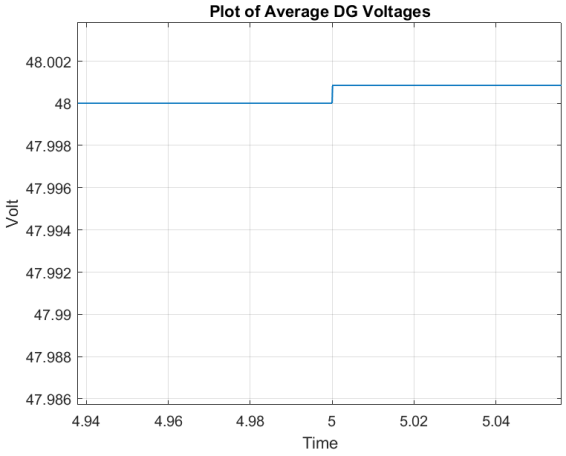


Figure B.16: Average voltage of perturbed system with $\mu = 2700$

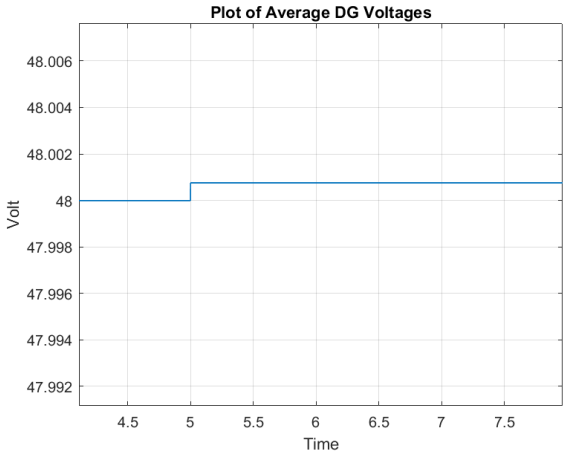


Figure B.17: Average voltage of perturbed system with $\mu = 3000$

The above figures recognizes that the tuning of $\mu$ will be off less influence when the tuning is defined above a specified threshold. Due to the significant small system responses in the above figures, the minimum threshold value is defined as $\mu = 3000$. This tuning value, combined with the significant tuning value of $\boldsymbol{\alpha}$ obtained in B, will then additionally satisfy the *Assumption* 4. Figure B.19 and B.20 shows that the control system is robust against cyber attacks disturbing the average voltage regulation when $\mu = 3000$, and the system is operating significantly close to the unforced system. However, the tuning of only the secondary control parameter destroys the system's ability to achieve consensus as portrait in B.20. The *Assumption* 4 regarding the combined tuning of $\boldsymbol{\alpha}$ and $\mu$ is therefore emphasized and the associated resilience simulations of this thesis, conducted for the different perturbed systems, are therefore based on the minimum tuning values of $2\boldsymbol{\alpha} = 6000 \rightarrow \boldsymbol{\alpha} = 3000$ and $\mu = 3000$.

Figure B.18: Minimum value of secondary control parameter

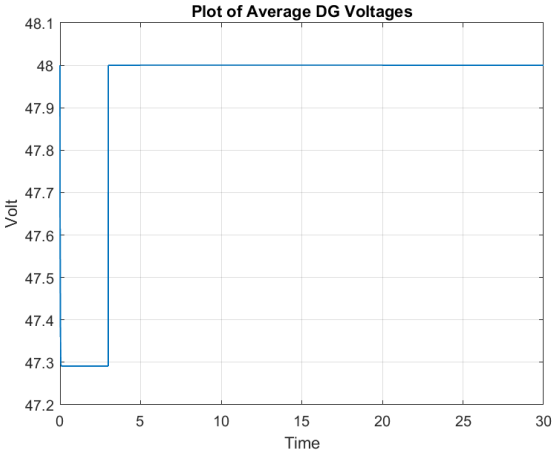


Figure B.19: Average voltage of perturbed system with $\mu = 3000$

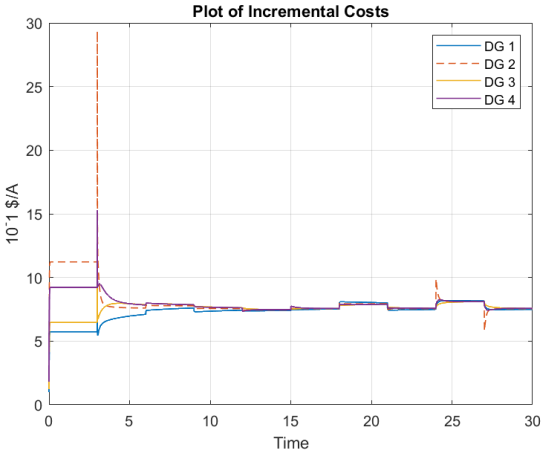


Figure B.20: Incremental costs of perturbed system with $\mu = 3000$

# C Simulations of Unforced System with Modified Controller

When the various simulations of systems with the modified controller are carried out, the implemented new dynamics is firstly tested in Simulink for the unforced system. The intention is to see that the new system modifications are correctly implemented. The tuning of $\mu$ is firstly defined equal to one: i.e., $\zeta = \frac{1}{\mu} = \frac{1}{1}$. The modified controller is then correctly implemented if the system response are behaving equally as the for the unforced system with the passivity based PI-controller.

Figure C.1: Unforced MG with Modified Distributed Controller

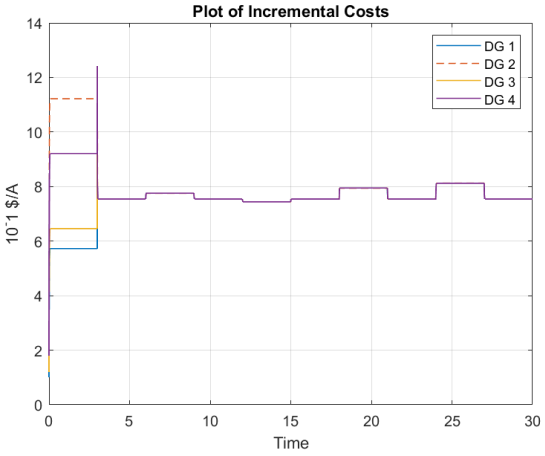


Figure C.2: Incremental costs of unforced system with control modifications

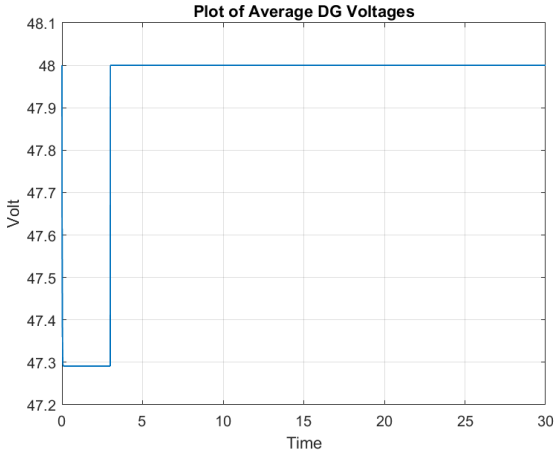


Figure C.3: Average voltage of unforced system with control modifications

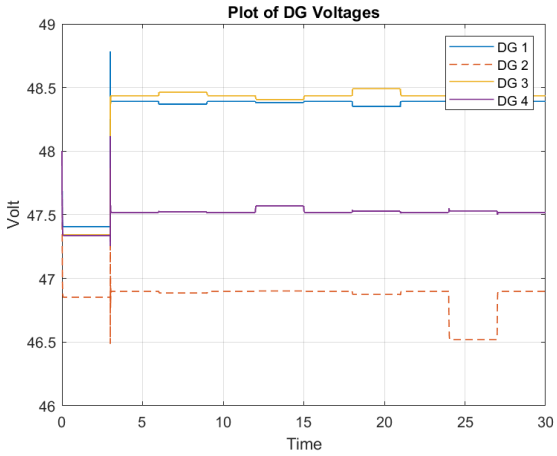


Figure C.4: DG voltages of unforced system with control modifications

Figure C.2, C.3 and C.4 displays identical system responses as the unforced system simulated in Section 4. It is then validated that the modified controller is implemented correctly and the simulations of the potential cyber attack attacks may be added accordingly.

## Simulating the Untuned and Modified Controller for the Perturbed Systems Exposed to Cyber Attacks

The system with modified controller and potential attacks is tested without tuning of the control parameters in order to examine if the controller and attack are correctly implemented. The two figures below features the same system response as the system with passivity based PI-controller exposed to cyber attack in the current sensors. Hence, the implementation of modified controller and cyber attacks are validated and the conclusion drawn when testing the resilience property is certified.

Figure C.5: Perturbed MG under CA2 with Control Modifications

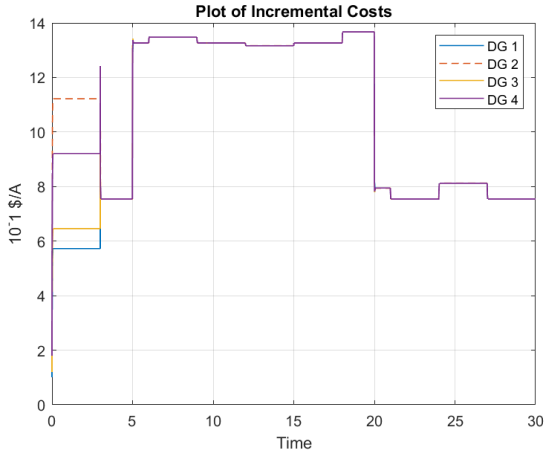


Figure C.6: Incremental costs of perturbed system with modified controller

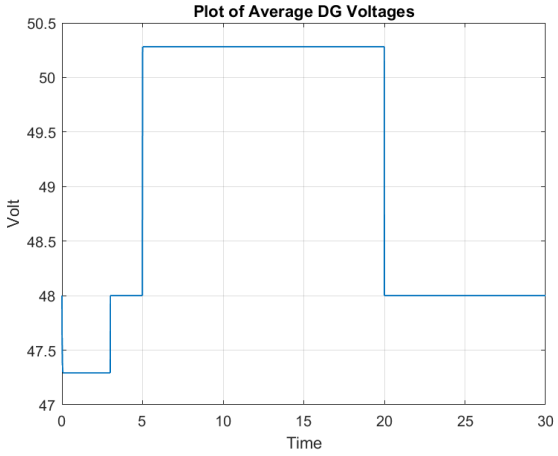


Figure C.7: Average voltage of perturbed system with modified controller

The two nest figures features the same system response as the system with passivity based PI-controller exposed to cyber attack in the communication links. Hence, the implementation of modified controller and cyber attacks are validated and the conclusion drawn when testing the resilience property is certified.

Figure C.8: Perturbed MG under CA3 with Control Modifications

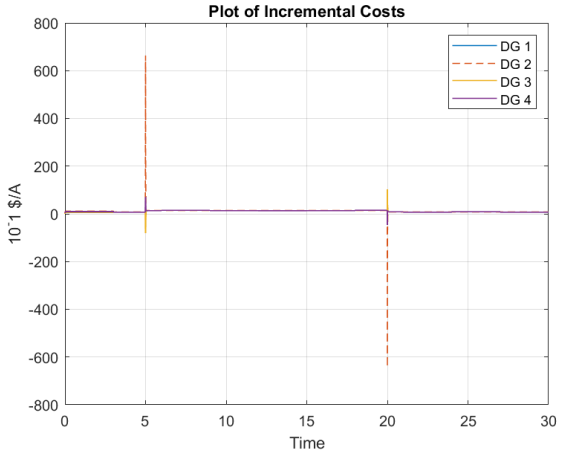


Figure C.9: Incremental costs of perturbed system with modified controller

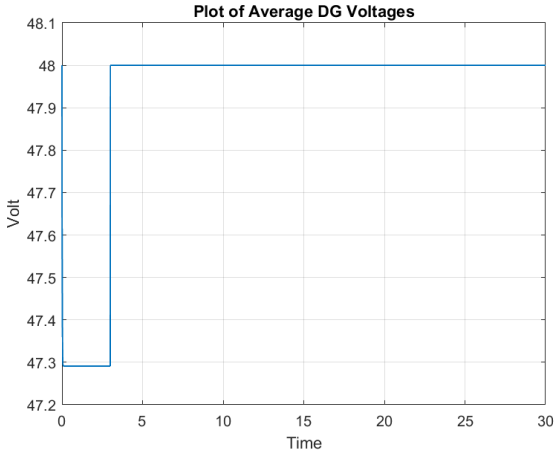


Figure C.10: Average voltage of perturbed system with modified controller

# D Lyapunov Stability Proofs

This section of the Appendix presents an overview of the Lyapunov stability proofs conducted in the associated specialization project. It is first proven that the droop controller ensures steady state operation at the minimum equilibrium of the electrical network: i.e., before the secondary controller is implemented. Further more, the Lyapunov stability proof of the cyber-physical MG: i.e., electrical network with interconnected secondary controller is presented. It is concluded that the closed loop control system still ensures global asymptotic stable operations of the MG, and the final generalized stability certificate is conducted.

## Droop Controlled Electrical Network

The stored energy of the electrical network is still designed based on incremental energy. This is the first step when designing the proposed Lyapunov function, influenced by the Hamiltonian of the electrical system. The incremental energy modelling ensures that the converged equilibrium of the Lyapunov function will be at the minimum value of the energy-function. The Lyapunov function and time derivative of the Lyapunov function is expressed below at the incremental level:

$$V_{tot}(\tilde{x}_{tot}) = \frac{1}{2}\tilde{x}^\top Q_{tot}\tilde{x} \tag{D.1}$$

$$\dot{\mathbf{V}}_{tot}(\tilde{\mathbf{x}}_{tot}) = \boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot}) \cdot \dot{\tilde{\mathbf{x}}}_{tot} \tag{D.2}$$

$$= \boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{F}_{tot}\boldsymbol{\nabla}\mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot}) \tag{D.3}$$

$$= \boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{J}_{tot}\boldsymbol{\nabla}\mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot}) - \boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{R}_{tot}\boldsymbol{\nabla}\mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot}) \tag{D.4}$$

The first term in the last equation represents the power preservation and the second term represents the dissipation. The first term is equal to zero as the energy always is conserved with respect to time. Hence, the total change in energy equals the dissipation of the system $\dot{\mathbf{V}}_{tot}(\tilde{\mathbf{x}}_{tot}) = -\boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{R}_{tot}\boldsymbol{\nabla}\mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})$.

The next step is then to assess the stability of the closed loop of the droop controlled power system. From the definition of global asymptotic stability presented in Khalil's book *Nonlinear systems* [25], the first step is to define that the stored incremental energy: i.e., the total Lyapunov function is positive definite. The Lyapunov function is dependent of second order states and the $Q_{tot}$ matrix: i.e., the function is positive definite depending on the $Q_{tot}$ matrix. As the matrix only contains stored inductance and capacitance $Q_{tot}$ is positive definite and the Lyapunov function is proven positive definite, $V(\tilde{x}_{tot}) > 0$. The function is also assessed with respect to the steady state equilibrium point, $V(\bar{x})$. $x = \bar{x}$ is defined as the constant state variables bringing the energy of the system to zero. Hence, the definition $V(\bar{x}) = 0$ is valid as the stored energy is equal to zero at the equilibrium point.

The Lyapunov function is then assessed with respect to the global stability criteria. $\dot{\mathbf{V}}(\tilde{\mathbf{x}}_{tot}) \leq 0$ is valid as the equations show that the stored energy with respect to time only depends on the dissipation. $\dot{\mathbf{V}}(\bar{\mathbf{x}}) = 0$ is always a valid property as the energy always converges to zero at the equilibrium point as $\bar{\mathbf{x}}$ is defined as the operational state bringing the time-dependent states to zero: i.e., steady state. Hence, it is proven that $\mathbf{x}$ needs to be equal to $\bar{\mathbf{x}}$ in order to achieve $\dot{\mathbf{V}}(\bar{\mathbf{x}}) = 0$ and the global stability criteria are now satisfied.

In order to ensure global and asymptotic stability La Salle's invariance theorem is applied on the Lyapunov function assessing what $\mathbf{x}$ needs to be in order to ensure steady state: i.e., when the time derivative of the stored energy goes to zero, $\mathbf{V}(\tilde{\mathbf{x}}) = 0$. If it is proven that $\mathbf{x} = \bar{\mathbf{x}}$ brings the system to equilibrium then the system converges to the assignable equilibrium point and GAS is proven satisfied for for the electrical droop controlled power system.

$$\dot{\mathbf{V}}(\tilde{x}) = 0 \rightarrow -\boldsymbol{\nabla}^\top \mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{R}_{tot}\boldsymbol{\nabla}\mathbf{V}_{tot}(\tilde{\mathbf{x}}_{tot}) = 0 \tag{D.5}$$

$$\rightarrow -\tilde{\mathbf{x}}^\top \mathbf{Q}_{tot}\mathbf{R}_{tot}\tilde{\mathbf{x}}\mathbf{Q}_{tot} = 0 \tag{D.6}$$

Both $\mathbf{R}_{tot}$ and $\mathbf{Q}_{tot}$ is positive definite and respectively has the property of being of full rank and quadratic. Hence, the change in the Lyapunov function equals to zero when $\tilde{\mathbf{x}} = 0$. The incremental state is defined as $\tilde{\mathbf{x}} = \mathbf{x} - \bar{\mathbf{x}}$ which then proves that the system converges to a non-trivial equilibrium point and is global asymptotic stable when $\mathbf{x} = \bar{\mathbf{x}}$. Hence, the asymptotic stability property $\dot{\mathbf{V}}(\tilde{\mathbf{x}}_{tot}) < 0$ is now concluded.

## Closed Loop Cyber-Physical MG with Secondary Controller

The stability proof of the cyber-physical MG with distributed control configurations are then conducted. The same approach as presented above is applied, however, the proposed Lyapunov function– and associated time derivative function – will now have additional terms related to the secondary controller. The proposed Lyapunov function is defined in the thesis and again presented below, influenced by the stored energy in the two networks brought to the incremental level.

$$V_T(\tilde{x}_T) = \mathbf{H}_{tot}(\tilde{\mathbf{x}}_{tot}) + \mathbf{H}_c(\tilde{\mathbf{x}}_c)$$

$$= \frac{1}{2}\tilde{\mathbf{x}}_{tot}^\top \mathbf{Q}_{tot}\tilde{\mathbf{x}}_{tot} + \frac{1}{2}\tilde{\mathbf{x}}_c^\top \mathbf{K}_I^{-1}\tilde{\mathbf{x}}_c \tag{D.7}$$

$$\dot{\mathbf{V}}_T(\tilde{\mathbf{x}}_T) = -\boldsymbol{\nabla}^\top \mathbf{H}_{tot}(\tilde{\mathbf{x}}_{tot})\mathbf{T}_T\boldsymbol{\nabla}^\top \mathbf{H}_{tot}(\tilde{\mathbf{x}}_{tot}) \tag{D.8}$$

The Lyapunov function candidate is proven positive definite, $V_T(\tilde{x}_T) > 0$ as energy is always preserved. Assessing the energy storage function with respect to the equilibrium point gives $V(\bar{x}_T) = 0$ as $\bar{x}_T$ is defined as the state variables bringing the energy to zero.

The change in energy is then assessed in order to conclude on global stability. $\dot{\mathbf{V}}(\tilde{\mathbf{x}}_T) \leq 0$ as the incremental energy function only depends on the dissipation of the system: i.e., it is converging against the minimum value. $\mathbf{T}_T = \text{blockdiag}((\mathbf{R}^{\mathcal{G}} + \mathbf{R}^D + \mathbf{r}), \mathbf{R}^{\mathcal{E}}, \mathbf{G}^{\mathcal{N}}_{cte}) \in \mathbb{R}^{3\times3}$ represented the dissipation matrix of the closed loop system: i.e., with the added dissipation of the secondary controller, where all the intrinsic matrices of $\mathbf{T}_T$ are defined positive definite. In order to achieve global stability the change in energy at the equilibrium point is assessed. $\dot{\mathbf{V}}(\bar{\mathbf{x}}_T) = 0$ is only valid when $\mathbf{x} = \bar{\mathbf{x}}$ and the system is able to achieve steady state at the minimum value of interest, $\mathbf{x}$.

Applying La Salle's argument to ensure asymptotic stability by assessing the state variables at the system minimum, $\dot{\mathbf{V}}_T(\tilde{\mathbf{x}}_T) = 0$. $\mathbf{T}_T$ is of full rank, $\mathbf{Q}_{tot}$ is quadratic, and $\dot{\mathbf{V}}_T(\tilde{\mathbf{x}}_T)$ is then equal to zero if the state variables, $\tilde{\mathbf{x}}_{tot}$, is zero. $\tilde{\mathbf{x}}_{tot}$ is equal to zero when $\mathbf{x}_{tot} = \bar{\mathbf{x}}_{tot}$ and it is proven that the minimum of the Lyapunov function is equal to operating point of interest. Thus, it is proven that the cyber-physical MG with distributed controller achieved global asymptotic stability.

# E Additional Theory Supporting the Master Thesis

## Passive Systems

In the assessment of physical systems, the concept of stored energy is often used to understand the functionality and behaviours of the system. Passive electrical systems are defined if the energy absorbed by external parts– over any time period– is greater than or equal to the increase in the stored energy over the same period [25]. This property can be viewed as an extension of the Lyapunov function for open systems later used to define and implement a passivity based controller that brings the system to stability at an assignable equilibrium point.

When the stability of a passive electrical system is analysed, the assessment is done on an open loop control system: i.e., with an undefined control value $u$. The system will then depend on two variables, the state variables $x$ and the control values $u$. The linear time invariant system $f(x) = Ax + Bu$ is then defined as $f(x, u) = Ax + Bu(x)$ with the associated passive output $y = Cx$. The steady state equilibrium point is then defined in E.1 where $\mathcal{E}$ is the set of admissible equilibrium points [25]:

$$\mathcal{E} = \left\{ x, u \middle| 0 = f(x, u) \right\} \qquad \bar{x}, \bar{u} \in \mathcal{E} \tag{E.1}$$

The Lyapunov theorem is also defined for passive systems using the a storage function $V(x)$. If the time derivative of the storage function, $\dot{V}(x)$, is less or equal to the product of the power input and the power output, then the system is passive:

$$\dot{V}(x) \leq \text{dissipation} + y^T u$$

If the loop is closed,: i.e., the control value is defined then $u \to u(x)$. The system $f(x, u(x))$ will not have a passive output and the storage function only depend on the energy dissipation:

$$\dot{V}(x) \leq \text{dissipation}$$

**Passivity Based Controller**
Passive systems can be made globally asymptotic stable if the implemented controller is designed from the passivity based methodology. This thesis focuses on designing a passivity based controller (PBC) defined from the passive output of the system. The objective is to design the controller that brings the system to steady state at an operating point of interest: i.e., interested in operating the system around a non-zero equilibrium point [26]. To achieve this control objective this thesis uses the procedure of incremental energy modelling describing the dynamics of the system as the deviation of the values in the wanted operating point and the values at the zero-equilibrium point $\tilde{(\cdot)} = (\cdot) - \bar{(\cdot)}$ [26]. $\bar{x}$ is the system state values at the equilibrium point and $\bar{u}$, $\bar{y}$ is the associated input and output related to the equilibrium point. When using the incremental system dynamics in the design of the controller, the question of whether the property of the original system is inherited by the incremental model will arise [26]. Hence, passivity is used to ensure that the proposed incremental controller brings the original system to steady state at the assignable equilibrium point.

## Consensus Protocol Based on the Laplacian Matrix

An overview of the consensus protocol is given in this section. The protocol contributes to find the optimal operating point with respect to the control objective. In order to achieve this value, two types of cooperative work can be applied, *leaderless consensus* or *leader-following consensus* [2], this thesis will focus on the leaderless consensus protocol.

**Leaderless consensus protocol**
Consensus is achieved when all the states have converged to the same value. The problem is based on the initial state of the nodes and the leaderless cooperative problem is also defined as *average consensus problem*. The consensus criteria is defined in E.2 where the node $\mathcal{N}_i$ will agree with node $\mathcal{N}_j$ when the criteria is valid [2].

$$\lim_{t\to\infty}(x_i(t)-x_j(t))=0 \qquad i\neq j \qquad \forall i,j\in\mathbb{N}^* \tag{E.2}$$

The state of the nodes, $x$ , depends on the model of the systems and for this thesis, and for simplicity, the states are assumed to have first order integrator dynamics. Also, the system is linear and therefore the system can be formulated as in E.3 where the control input of the node, $u_i(t)$, is related to the local state in discrete time [2].

$$\dot{x}_i = u_i(t) \rightarrow x_{k+1}-x_k = u_k \rightarrow x_{k+1} = u_k + x_k \tag{E.3}$$

Applying a simple consensus protocol based on graph theory with an arbitrary directed graph topology is presented in E.4. A preposition of a control law closing the control loop is then defined when assuming that the nodes instantaneously exchange information.

$$\begin{aligned} u_i(t) = -\sum_{k\sim\mathcal{N}} a_{ik}(x_k-x_i) &= (\sum_{k\sim\mathcal{N}} a_{ik}x_k) - (\sum_{k\sim\mathcal{N}} a_{ik})x_i \\ &= (Ax)_i - (D_{ii})x_i \end{aligned} \tag{E.4}$$

The local states of the node $i$ and node $j$ is represented as $x_i$ and $x_j$ respectively [2]. $(x_j - x_i)$ will then represent the change in the state variables between the two connected nodes: i.e., the neighbour error containing the difference in the exchanged values. The total system is then written in E.5 using matrix notation with respect to the neighbouring units.

$$\dot{x}(t) = u(t) = \mathcal{A}x(t) - \mathcal{D}x(t) = -(\mathcal{D}-\mathcal{A})x(t) = -\mathcal{L}x(t) \tag{E.5}$$

**Properties of the leaderless consensus protocol**
When the system is modelled with an undirected graph: i.e., $a_{ik} = a_{ki}$, then the sum of all the states of all the nodes is a time invariant value as shown in E.6 [2]. This will be valid because of the property of the Laplacian where all rows add to zero.

$$\mathbf{1}_n^\top \dot{\mathbf{x}} = -(\mathbf{1}_n^\top \mathcal{L}x) = 0 \tag{E.6}$$

$$\frac{d}{dt}\sum_{i=1}^{n} x_i(t) = 0 \rightarrow \sum_{i=1}^{n} x_i(t) = \text{constant} \tag{E.7}$$

## Positive Definite Proof of the Laplacian Matrix

The *Gershgorin Circle Theorem*, defined in E.8, describes smaller regions where each eigenvalue of the system is located. The diagonal elements of the Laplacian represents a center of an associated circle with a diameter equal to the absolute value of the sum of the non-diagonal elements in each row. Given the definition of an arbitrary Laplacian matrix, the centre needs to be $\geq 0$ with a diameter $\leq$ the diagonal element. Hence, the circles defining the regions where the eigenvalues are located, has a centre-value $\geq 0$ with circle-periphery only containing elements $\geq 0$. The Laplacian is therefore always positive semidefinite with eigenvalues in the right half plane [27].

$$\begin{aligned} &\text{If} \quad \mathcal{L}\in\mathbb{C}^{n\times n} \quad \text{then,} \\ &\sigma(L)\subseteq\mathcal{S}_\mathcal{R} = \bigcup_{i=1}^{n}\mathcal{R}_i, \qquad \mathcal{R}_i = \{z\in\mathbb{C} : |z-l_{ii}| \leq \sum_{\substack{j=1\\ j\neq i}}^{n} |l_{ij}|\} \end{aligned} \tag{E.8}$$

The Laplacian is therefore always defined as positive semidefinite as presented below, verified with the properties of a square matrix defined in E and the *Gershgorin Circle Theorem.*

$$Z^\top \mathcal{L} Z \geq 0 \qquad \forall Z \in \mathbb{R}^n \tag{E.9}$$

## Useful Properties of Square Matrices

It is useful to show that the positive definiteness of the Laplacian can be assessed by studying the symmetrical part of the matrix even if the Laplacian is not fully symmetric. The Laplacian is defined as a square matrix and one useful property of square matrices is, in this section, presented by using a trivial square matrix $\mathbf{A}$. The matrix is first defined as the summation of its symmetrical and skew-symmetrical parts: $\mathbf{A} = \mathbf{A}_{sym} + \mathbf{A}_{skew}$ with the associated symmetric and skew-symmetrical definitions:

$$\mathbf{A}_{skew} = \frac{1}{2}(\mathbf{A} - \mathbf{A}^T)$$
$$\mathbf{A}_{sym} = \frac{1}{2}(\mathbf{A} + \mathbf{A}^T)$$

When multiplying a symmetric matrix, $\mathbf{Z}$, on both sides of a skew-symmetric matrix as done in E.10 it can be shown that the product is equal to zero, showing that the property of the square matrix is only depend on the property of the symmetrical part.

$$\begin{aligned} \mathbf{Z}^\top \mathbf{A}_{skew} \mathbf{Z} &= \frac{1}{2}\mathbf{Z}^\top \mathbf{A}\mathbf{Z} - \frac{1}{2}\mathbf{Z}^\top \mathbf{A}^\top \mathbf{Z} \\ &= \frac{1}{2}\mathbf{Z}^\top \mathbf{A}\mathbf{Z} - \frac{1}{2}\mathbf{Z}^T \mathbf{A}\mathbf{Z} = 0 \end{aligned} \tag{E.10}$$

Hence, it is shown that the square $\mathbf{A}$-matrix can be proven positive definite by assessing only the symmetrical part. This proof is valid for any square matrix, and it is then proven that the relation in E.9 is valid even if the Laplacian is not a symmetric matrix, since the positive definite symmetrical part defines the definite property of the Laplacian [2].

## Region of Attraction

When the Lyapunov's method is applied, the defined domain $D \subset \mathbb{R}^n$ is not necessary equal to the region of attraction in which the global asymptotic stability is ensured. In *Lemma 3.2* in Khalil's Nonlinear Control [23] the region of attraction is specified as follows: *The region of attraction of an asymptotically stable equilibrium point is an open, connected invariant set, and its boundary is formed by trajectories*[23] . Hence, the region of attraction needs to be defined as a subset of $D$ with a smaller bound $c$ so that the Lyapunov function is certified to always converge to the equilibrium within that bounded region. The region of attraction is then defined as the bounded open set $\Omega_c = \{V(x) < c\} \subset D$ and $D = \{\| \ x \ \| < r\}$. Hence, $\Omega_c$ is bounded and contained in $D$ when $c > 0$ and non-infinite. We are then interested in the largest set $\Omega_c$, that is the largest value for the constant $c$ in order to conclude that the Lyapunov function always converges to the equilibrium when all $x \in \Omega$. We can ensure that $\Omega_c \subset D$ by choosing:

$$c < \min_{\|x\|=r} V(x) = \min_{\|x\|=r} x^\top P x = \lambda_{min}(P) r^2 \tag{E.11}$$

$P$ is a positive definite matrix defined as real symmetric matrix if all eigenvalues are positive and the Lyapunov function $V(x)$ is defined by $x^\top P x$. A simple visualization of Lyapunov functions converging to the region of attraction, $\Omega_c$, with associated bound at the periphery, $c > 0$, defined as a subset of the domain, $D$, containing the orgin [23] as presented in Figure E.1.

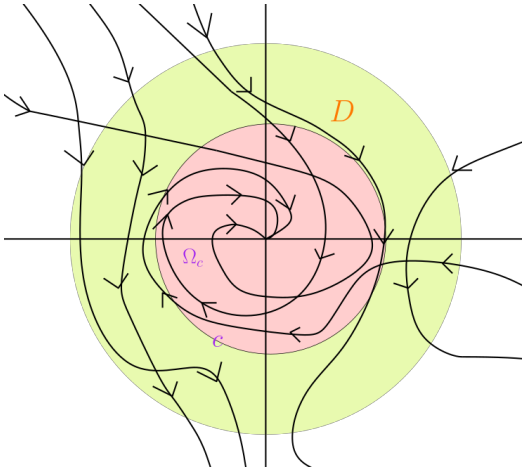


Figure E.1: Region of Attraction

Cornelia Skaga

Energy Control of Complex Cyber-Physical Microgrids: Robustness against Cyber Attacks

NTNU
Norwegian University of
Science and Technology