



Delft University of Technology

#### Document Version

Final published version

#### Citation (APA)

Rajkumar , V. (2025). *Cyber Security of Power Systems: Dynamical Analysis of Cascading Failures and Defense: How the bits and bytes can influence the volts and the amps*. [Dissertation (TU Delft), Delft University of Technology]. <https://doi.org/10.4233/uuid:7d2d7d84-61b0-469b-b2d0-a1a00f88f83e>

#### Important note

To cite this publication, please use the final published version (if applicable).  
Please check the document version above.

#### Copyright

In case the licence states "Dutch Copyright Act (Article 25fa)", this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.  
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

#### Sharing and reuse

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

#### Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.  
We will remove access to the work immediately and investigate your claim.

*This work is downloaded from Delft University of Technology.*

# Cyber Security of Power Systems:

## Dynamical Analysis of Cascading Failures and Defense

*How the bits and bytes can influence the volts and the amps*

Vetrivel RAJKUMAR



# **Cyber Security of Power Systems: Dynamical Analysis of Cascading Failures and Defense**

How the bits and bytes can influence the volts and the amps



# **Cyber Security of Power Systems: Dynamical Analysis of Cascading Failures and Defense**

How the bits and bytes can influence the volts and the amps

## **Dissertation**

for the purpose of obtaining the degree of doctor  
at Delft University of Technology,  
by the authority of the Rector Magnificus prof. dr. ir. T.H.J.J. van der Hagen,  
Chair of the Board for Doctorates  
to be defended publicly on  
Tuesday 9 September 2025 at 17:30 o'clock

**Vetrivel RAJKUMAR**

Master of Science in Electrical Engineering,  
Delft University of Technology, Netherlands  
born in Chennai, Tamil Nadu, India.

The dissertation has been approved by the promotor.

Promotors: Prof. Dr. P. Palensky, Dr. Dipl.-Ing. J. L. Rueda Torres

Copromotor: Dr. A.I. Ştefanov

Composition of the doctoral committee:

|                                   |                                            |
|-----------------------------------|--------------------------------------------|
| Rector Magnificus,                | Chairperson                                |
| Prof. Dr. P. Palensky,            | Delft University of Technology, promotor   |
| Dr. Dipl.-Ing. J. L. Rueda Torres | Delft University of Technology, promotor   |
| Dr. A.I. Ştefanov,                | Delft University of Technology, copromotor |

*Independent members:*

|                          |                                                |
|--------------------------|------------------------------------------------|
| Prof. Dr. Ir. M. Popov,  | Delft University of Technology                 |
| Prof. Dr. A. Srivastava, | West Virginia University                       |
| Dr. S. Lakshminarayana,  | University of Warwick                          |
| Dr. T. Strasser,         | Austrian Institute of Technology               |
| Prof. Dr. A. Smets,      | Delft University of Technology, reserve member |

This research was funded under the European Community's Horizon 2020 Program (H2020/2014-2020) in project "ERIGrid 2.0" with Grant Agreement No. 870620.



*Keywords:* cascading failures, cyber security, cyber resilience, digital substation, power system dynamics

*Printed by:* ProefschriftMaken

*Cover:* Vetrivel Rajkumar (GPT-5)

*Style:* TU Delft House Style, with modifications by Moritz Beller  
<https://github.com/Inventitech/phd-thesis-template>

ISBN 978-94-6384-842-8

An electronic version of this dissertation is available at  
<https://repository.tudelft.nl/>.

*“Deep in the human unconscious is a pervasive need for a logical universe that makes sense.  
But the real universe is always one step beyond logic.”*

– from the sayings of Muad'Dib by the Princess Irulan, *Dune*



# Contents

|                                                                                     |             |
|-------------------------------------------------------------------------------------|-------------|
| <b>Nomenclature</b>                                                                 | <b>xi</b>   |
| <b>Summary</b>                                                                      | <b>xiii</b> |
| <b>Samenvatting</b>                                                                 | <b>xv</b>   |
| <b>Acknowledgments</b>                                                              | <b>xix</b>  |
| <b>List of Publications</b>                                                         | <b>xxi</b>  |
| <b>1 Introduction</b>                                                               | <b>1</b>    |
| 1.1 Background and Motivation . . . . .                                             | 2           |
| 1.2 Power Grid Digitalization and Cyber Security . . . . .                          | 2           |
| 1.3 State-of-the-Art . . . . .                                                      | 3           |
| 1.3.1 Cascading Failure Analysis Methods . . . . .                                  | 3           |
| 1.3.2 Cyber Security for Power Grids . . . . .                                      | 4           |
| 1.4 Research Gaps . . . . .                                                         | 5           |
| 1.5 Overall Thesis Objective and Research Questions. . . . .                        | 6           |
| 1.6 Methods/Approaches. . . . .                                                     | 6           |
| 1.7 Scientific Contributions . . . . .                                              | 9           |
| 1.8 Thesis Outline . . . . .                                                        | 10          |
| <b>2 Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures</b> | <b>13</b>   |
| 2.1 Introduction . . . . .                                                          | 14          |
| 2.1.1 Cascading Failures and Blackouts . . . . .                                    | 14          |
| 2.1.2 Modelling of Cascading Failures . . . . .                                     | 15          |
| 2.1.3 Cyber Security of Power Grids . . . . .                                       | 15          |
| 2.1.4 Review of State-of-The-Art . . . . .                                          | 16          |
| 2.2 Review of Historical Blackouts . . . . .                                        | 17          |
| 2.2.1 Italy, 2003 . . . . .                                                         | 17          |
| 2.2.2 USA-Canada, 2003 . . . . .                                                    | 17          |
| 2.2.3 Europe, 2006 . . . . .                                                        | 18          |
| 2.2.4 India, 2012 . . . . .                                                         | 18          |
| 2.2.5 Turkey, 2015 . . . . .                                                        | 18          |
| 2.2.6 United Kingdom, 2019 . . . . .                                                | 19          |
| 2.2.7 Pakistan, 2021 . . . . .                                                      | 19          |
| 2.2.8 Summary. . . . .                                                              | 19          |
| 2.3 Connection Between Cascading Failures and Cyber Security . . . . .              | 20          |
| 2.3.1 Cyber-Physical Factors . . . . .                                              | 21          |

|          |                                                                                      |           |
|----------|--------------------------------------------------------------------------------------|-----------|
| 2.4      | Cyber Attacks Enabling Cyber-Physical Factors . . . . .                              | 26        |
| 2.4.1    | Cyber Kill Chain . . . . .                                                           | 26        |
| 2.4.2    | Malware Attack . . . . .                                                             | 27        |
| 2.4.3    | Operational Technology Hijacking . . . . .                                           | 28        |
| 2.4.4    | False Data Injection . . . . .                                                       | 29        |
| 2.4.5    | Advanced Persistent Threats . . . . .                                                | 32        |
| 2.5      | Conclusions . . . . .                                                                | 33        |
| <b>3</b> | <b>Cyber Security of Digital Substations: Impact Analysis and Mitigation</b>         | <b>35</b> |
| 3.1      | Introduction . . . . .                                                               | 36        |
| 3.2      | Power System Protection and Automation . . . . .                                     | 36        |
| 3.2.1    | Distance Protection . . . . .                                                        | 36        |
| 3.2.2    | Out of Step Protection . . . . .                                                     | 36        |
| 3.2.3    | Frequency and Voltage Protection . . . . .                                           | 37        |
| 3.3      | IEC 61850 Standard. . . . .                                                          | 37        |
| 3.3.1    | Generic Object Oriented Substation Event . . . . .                                   | 38        |
| 3.3.2    | Sampled Values . . . . .                                                             | 39        |
| 3.3.3    | Security Vulnerabilities . . . . .                                                   | 39        |
| 3.3.4    | State-of-the-Art . . . . .                                                           | 40        |
| 3.4      | Cyber Attack Model . . . . .                                                         | 41        |
| 3.4.1    | Network Reconnaissance. . . . .                                                      | 41        |
| 3.4.2    | Cyber Attack Execution . . . . .                                                     | 42        |
| 3.5      | Cyber Attack Proof-of-Concept . . . . .                                              | 44        |
| 3.5.1    | GOOSE Spoofing. . . . .                                                              | 44        |
| 3.5.2    | Hardware-in-the-Loop Setup. . . . .                                                  | 45        |
| 3.6      | Impact on Power System. . . . .                                                      | 47        |
| 3.6.1    | Impact of GOOSE spoofing on 5-Bus Test System . . . . .                              | 47        |
| 3.6.2    | Impact of GOOSE Attack on 9-bus Test System. . . . .                                 | 49        |
| 3.6.3    | Impact of SV replay attack . . . . .                                                 | 49        |
| 3.7      | Cyber Security of IEC 61850 GOOSE . . . . .                                          | 50        |
| 3.7.1    | IEC 62351-6 Standard. . . . .                                                        | 51        |
| 3.7.2    | Related Work. . . . .                                                                | 51        |
| 3.7.3    | Cyber Security of GOOSE Messages . . . . .                                           | 52        |
| 3.8      | HMAC Implementation . . . . .                                                        | 52        |
| 3.8.1    | HMAC Calculation. . . . .                                                            | 52        |
| 3.8.2    | Architecture . . . . .                                                               | 53        |
| 3.9      | Results of HMAC Implementation . . . . .                                             | 54        |
| 3.9.1    | GOOSE Message with HMAC Extension . . . . .                                          | 54        |
| 3.9.2    | Performance Evaluation . . . . .                                                     | 55        |
| 3.10     | Concluding Remarks . . . . .                                                         | 58        |
| <b>4</b> | <b>Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks</b> | <b>59</b> |
| 4.1      | Motivation . . . . .                                                                 | 60        |
| 4.2      | State-of-the-Art . . . . .                                                           | 60        |

|          |                                                                    |            |
|----------|--------------------------------------------------------------------|------------|
| 4.3      | Cyber-Physical Attacks on Power Grids . . . . .                    | 61         |
| 4.3.1    | Spoofing Attacks . . . . .                                         | 61         |
| 4.3.2    | Switching Attacks . . . . .                                        | 62         |
| 4.3.3    | Data Integrity Attacks . . . . .                                   | 62         |
| 4.3.4    | Cyber-Physical Attacks . . . . .                                   | 62         |
| 4.4      | Dynamical Analysis of Cascading Failures . . . . .                 | 63         |
| 4.4.1    | Power System Dynamics . . . . .                                    | 63         |
| 4.4.2    | Time-Frequency Analysis . . . . .                                  | 64         |
| 4.4.3    | Instantaneous Damping Correlation . . . . .                        | 65         |
| 4.4.4    | Point of No Return and Singular Value Decomposition . . . . .      | 66         |
| 4.5      | Experimental Results . . . . .                                     | 69         |
| 4.5.1    | Cascading Failure Simulations . . . . .                            | 69         |
| 4.5.2    | Point-of No-Return Identification . . . . .                        | 78         |
| 4.5.3    | Acceleration Mechanism . . . . .                                   | 81         |
| 4.6      | Conclusions . . . . .                                              | 85         |
| <b>5</b> | <b>Preventive Controlled Islanding For Cyber Resilience</b>        | <b>87</b>  |
| 5.1      | Motivation . . . . .                                               | 88         |
| 5.2      | Physics-Informed Graph Convolution Network . . . . .               | 89         |
| 5.2.1    | Architecture . . . . .                                             | 89         |
| 5.2.2    | Weight Adjustment for Isolation of Vulnerable Substations. . . . . | 90         |
| 5.2.3    | Loss Function and Constraints . . . . .                            | 90         |
| 5.2.4    | Training and Clustering . . . . .                                  | 91         |
| 5.3      | Experimental Results . . . . .                                     | 91         |
| 5.3.1    | Case Studies . . . . .                                             | 91         |
| 5.3.2    | Dynamical Analysis of Preventive Islanding . . . . .               | 92         |
| 5.4      | Conclusions . . . . .                                              | 96         |
| <b>6</b> | <b>Conclusions and Discussion</b>                                  | <b>97</b>  |
| 6.1      | Answers to Research Questions . . . . .                            | 97         |
| 6.2      | Recommendations and Future Work . . . . .                          | 101        |
|          | <b>Bibliography</b>                                                | <b>105</b> |



# Nomenclature

**AES** Advanced Encryption Standard

**AVR** Automatic Voltage Regulator

**DOS** Denial-of-Service

**ENTSO-E** European Network of Transmission System Operators for Electricity

**FDI** False Data Injection

**GCN** Graph Convolutional Network

**GOOSE** Generic Object Oriented Substation Event

**GMAC** Galois Message Authentication Code

**HIL** Hardware-in-the-Loop

**HMAC** Hash-based Message Authentication Code

**ICT** Information and Communication Technology

**IED** Intelligent Electronic Device

**MITM** Man-in-the-Middle

**OT** Operational Technology

**PNR** Point-of-No-Return

**RTDS** Real-Time Digital Simulator

**ROCOF** Rate-of-Change-of-Frequency

**SCADA** Supervisory Control and Data Acquisition

**SV** Sampled Values

**UFLS** Under Frequency Load Shedding

**UVLS** Under Voltage Load Shedding



# Summary

The increased digitalization of the power grid and transition to cyber-physical power systems raise serious concerns about cyber security and secure operation of the power system. It is now well recognized that information and communication technologies are vulnerable to cyber attacks. Thereby, electrical power grids as critical infrastructures are susceptible to cyber attacks as well. Malicious cyber attacks on power grid infrastructure can detrimentally affect power system operation and stability. In the worst-case, it can trigger cascading failures across the system, leading to a blackout. A coordinated cyber attack across multiple locations can collapse the entire interconnected power grids of nations, or even continents. This is a real modern-day threat, as seen during the cyber attacks on the Ukrainian power grid in 2015, 2016, and 2022. Therefore, power grid resilience and cyber security are now recognized challenges for power system operation and security of electricity supply. The gist of this entire thesis can be summarized as follows. *“Analyze and demonstrate how cyber attacks on power grids may cause and accelerate cascading failures. Based on this analysis, develop suitable proactive defense measures to contain the spread of cascading failures.”* Consequently, the core research focus of the thesis with a threefold objective is as follows:

## 1. Cyber security of digital substations

This thesis investigated the impact of cyber threats targeting digital substations. Experiments demonstrate the catastrophic impact of spoofing and replay attacks targeting Operational Technology (OT) protocols and standards used in digital substations, leading to relay denial-of-service and malfunction. Subsequently, it is experimentally shown how these events may snowball resulting in cascading failures and blackouts. Based on this analysis, this thesis developed mitigation measures based on IEC 62351-6 using Hash-based Message Authentication Code (HMAC) to secure critical control communications in digital substations, adherent to latency requirements of  $< 4ms$ . The aforementioned studies are conducted using a hardware-in-the-loop cyber-physical experimental framework that closely resembles real-world conditions within a digital substation, including intelligent electronic devices and protection schemes. Thus, the outcomes of this research are of particular importance to both, vendors and utilities.

## 2. Dynamical analysis of power system cascading failures caused by cyber attacks

This thesis proposed a data-driven method for dynamical analysis of power system cascading failures caused by cyberattacks. It provides experimental proof on how cyber attacks may accelerate the cascading failure mechanism, in comparison to historically observed blackouts. Using a dynamic power grid model, consisting of

multiple, coordinated protection schemes, the point of no return is defined and analysed in a cascading failure sequence by applying the Hilbert–Huang transform for time–frequency analysis. Numerical results indicate, cyber attacks may accelerate cascading failures at least by a factor of  $3\times$ . This is due to the excitation and non-damping of multiple frequency modes greater than 1 Hz in a short time span.

### 3. Defense against cyber attack induced cascading failures

Cyber-physical power systems are vulnerable to cyber attacks that may lead to cascading failures and power outages. A promising solution to tackle this emerging issue is the concept of preventive/proactive controlled islanding before the cyber event occurs based on early detection of cyber attacks. Hence, this thesis developed a novel physics-informed graph convolution network to perform preventive controlled islanding. By incorporating power system physics into the neural network loss function formulations, the resulting islands were made self-sufficient and voltage and frequency stable. Experimental simulations using a modified version of the IEEE 39-bus test system with coordinated protection schemes prove that the islands formed using the proposed method can contain the spread of cascading failures. This results in minimization of loss of load by up to 90% and 62% when single and multiple substations are compromised, respectively. Hence, this work paves the way towards automated cyber-resilience for power systems and provides system operators with decision making recommendations to curtail the spread of cascading failures.

This thesis addressed the increasingly crucial topic of cyber security for power systems. It provides a comprehensive analysis of how cyber attacks may trigger and accelerate cascading failures in power grids, potentially leading to large-scale power outages. Furthermore, this research enhances our understanding of power grid cyber resilience by experimentally demonstrating the vulnerabilities of digital substations, proposing a novel data-driven method for analysing cyber-induced cascading failures, and developing an advanced physics-informed graph convolutional network for preventive controlled islanding. The findings of this thesis are highly relevant to utilities and vendors, as they offer practical insights into the pitfalls associated with power system digitalization and possible adverse consequences. Thereby, the proposed cascading failure analysis technique and preventive islanding defense strategy directly contribute towards enhancing the cyber security of power systems and ensuring better preparedness in the face of the ever-growing cyber threat landscape. Ultimately, this research contributes to a more cyber secure and resilient power system.

# Samenvatting

De toenemende digitalisering van het elektriciteitsnet en de overgang naar cyberfysieke energiesystemen leiden tot ernstige zorgen over cyberveiligheid en een veilige werking van het energiesysteem. Systemen leiden tot ernstige zorgen over cyberveiligheid en een veilige werking van het elektriciteitssysteem. Het wordt nu algemeen erkend dat informatie- en communicatietechnologieën kwetsbaar zijn voor cyberaanvallen. Daardoor zijn elektriciteitsnetten als kritieke infrastructuren ook gevoelig voor cyberaanvallen. Kwaadaardige cyberaanvallen op de infrastructuur van het elektriciteitsnet kunnen de werking en stabiliteit van het elektriciteits- systeem nadelig beïnvloeden. de werking en stabiliteit van het elektriciteitsnet nadelig beïnvloeden. In het ergste geval kan dit leiden tot storingen in het hele systeem veroorzaken, wat kan leiden tot een black-out. Een gecoördineerde cyberaanval op meerdere locaties kan het hele onderling verbonden elektriciteitsnet van naties of zelfs continenten platleggen of zelfs continenten. Dit is een reële hedendaagse dreiging, zoals bleek tijdens de cyberaanvallen op het Oekraïense elektriciteitsnet in 2015, 2016 en 2022. Daarom zijn de veerkracht van het elektriciteitsnet en cyber veiligheid nu erkende uitdagingen voor de werking van het energiesysteem en de veiligheid van de elektriciteitsvoorziening. stroomvoorziening. De kern van dit hele proefschrift kan als volgt worden samengevat. “Analyseren en aantonen hoe cyberaanvallen op elektriciteitsnetten cascdestoringen kunnen veroorzaken en versnellen. Ontwikkel op basis van deze analyse geschikte proactieve verdedigingsmaatregelen om de verspreiding van cascdestoringen in te dammen.” De kern van het onderzoek in dit proefschrift met een driedelige doelstelling als volgt:

## 1. Digitale onderstationbeveiliging

Deze dissertatie onderzocht de impact van cyberbedreigingen gericht op digitale onderstations. Experimenten tonen de catastrofale impact aan van spoofing- en replay-aanvallen gericht op Operationele Technologie (OT)-protocollen en standaarden die worden gebruikt in digitale onderstations, wat leidt tot ontzegging van de dienst en storing van het relais. Vervolgens wordt experimenteel aangetoond hoe deze gebeurtenissen een sneeuwbal effect kunnen hebben met cascdestoringen en stroomstoringen tot gevolg. Op basis van deze analyse zijn in dit proefschrift mitigerende maatregelen ontwikkeld op basis van IEC 62351-6, waarbij gebruik wordt gemaakt van Hash-based Message Authentication Code (HMAC) om kritieke regelcommunicatie in digitale onderstations te beveiligen, met inachtneming van de latentievereisten van  $< 4$  ms. De bovengenoemde onderzoeken worden uitgevoerd met behulp van een hardware-in-the-loop cyberfysisch experimenteel kader dat de werkelijke omstandigheden in een digitaal onderstation, inclusief intelligente elektronische apparaten en beveiligingssystemen, goed benadert. De resultaten van dit onderzoek zijn dus van bijzonder belang voor zowel leveranciers als nutsbedrijven.

## **2. Dynamische analyse van cascdestoringen in elektriciteitssystemen veroorzaakt door cyberaanvallen**

In dit proefschrift wordt een datagestuurde methode voorgesteld voor de dynamische analyse van cascdestoringen in elektriciteitssystemen als gevolg van cyberaanvallen. Het biedt experimenteel bewijs voor hoe cyberaanvallen het mechanisme van cascdestoringen kunnen versnellen, in vergelijking met historisch waargenomen black-outs. Met behulp van een dynamisch elektriciteitsnetmodel, bestaande uit meerdere, gecoördineerde beveiligingssystemen, wordt het punt waarop geen terugkeer mogelijk is gedefinieerd en geanalyseerd in een cascade van storingen door de Hilbert-Huang-transformatie toe te passen voor tijdrequentieanalyse. Numerieke resultaten geven aan dat cyberaanvallen cascdestoringen minstens met een factor  $3\times$  kunnen versnellen. Dit komt door de opwinding en niet-damping van meerdere frequentiemodi groter dan 1 Hz in een korte tijdspanne.

## **3. Verdediging tegen cascdestoringen door cyberaanvallen**

Cyberfysieke elektriciteitssystemen zijn kwetsbaar voor cyberaanvallen die kunnen leiden tot cascdestoringen en stroomuitval. Een veelbelovende oplossing om dit opkomende probleem aan te pakken is het concept van preventieve/proactieve gecontroleerde eilandering voordat de cybergebeurtenis plaatsvindt op basis van vroege detectie van cyberaanvallen. Daarom is in dit proefschrift een nieuw fysica-geïnformeerd grafiekconvolutienetwerk ontwikkeld om preventieve gecontroleerde eilandvorming uit te voeren. Door de fysica van het elektriciteitssysteem op te nemen in de verliesfunctieformuleringen van het neurale netwerk, werden de resulterende eilanden zelfvoorzienend en stabiel wat betreft spanning en frequentie. Experimentele simulaties met een aangepaste versie van het IEEE 39-bus testsysteem met gecoördineerde beveiligingsschema's tonen aan dat de eilanden die met de voorgestelde methode zijn gevormd de verspreiding van cascdestoringen kunnen beperken. Dit resulteert in een minimalisatie van het verlies aan belasting tot 90% en 62% wanneer respectievelijk één en meerdere onderstations worden getroffen. Dit werk baant dus de weg naar geautomatiseerde cyberweerbaarheid voor elektriciteitssystemen en biedt systeembeheerders aanbevelingen voor besluitvorming om de verspreiding van cascdestoringen te beperken.

Deze dissertatie behandelt het steeds belangrijker wordende onderwerp van cyberveiligheid voor elektriciteitssystemen. Het biedt een uitgebreide analyse van de manier waarop cyberaanvallen cascdestoringen in elektriciteitsnetten kunnen veroorzaken en versnellen, wat mogelijk kan leiden tot grootschalige stroomuitval. Verder vergroot dit onderzoek ons begrip van de cyberweerbaarheid van elektriciteitsnetwerken door experimenteel de kwetsbaarheid van digitale onderstations aan te tonen, een nieuwe gegevensgestuurde methode voor te stellen voor het analyseren van cybergeïnduceerde cascdestoringen en een geavanceerd natuurkundig geïnformeerd grafisch convolutioneel netwerk te ontwikkelen voor preventieve gecontroleerde eilandvorming. De bevindingen van dit proefschrift zijn zeer relevant voor nutsbedrijven en verkopers, omdat ze praktische inzichten bieden in de valkuilen die gepaard gaan met de digitalisering van het energiesysteem en de mogelijke nadelige gevolgen. Daarbij dragen de voorgestelde cascadefoutenanalyse-techniek en de preventieve verdedigingsstrategie voor eilandbedrijf direct bij aan het

verbeteren van de cyberveiligheid van elektriciteitssystemen en zorgen ze voor een betere paraatheid ten opzichte van het steeds groter wordende cyberdreigingslandschap. Uiteindelijk draagt dit onderzoek bij aan een cyberveiliger en veerkrachtiger energiesysteem.



# Acknowledgments

Without a doubt, the acknowledgments are the most eagerly and widely read part of any thesis. This doctoral journey of the past 4-5 years has truly been a revelation. Starting a PhD in the middle of an ongoing global pandemic was challenging, to say the least. It feels just like yesterday when I decided to move to the Netherlands to pursue a master's that eventually culminated in this PhD. If someone had told me 8 years ago that I would "enjoy" cycling in the rain, constantly complain about the weather, and look forward to the (rare) sunny days, I would have laughed. Yet, here we are. My time in Delft has been a transformational one, both academically and personally and now I am also happy to officially be a "Delftenaar."

First and foremost, I would like to thank my entire supervisory team of Prof. Dr. Peter Palensky, Dr. Jose Rueda Torres, and Dr. Alex Ștefanov. Peter, thank you for providing me this opportunity to pursue a PhD within the scope of ERIGrid 2. Your leadership and empathy have gone a long way in the successful completion of my PhD. Thank you for all our discussions and brainstorming sessions that left me feeling full of ideas and energy. You are truly symbolic of the "mad scientist." I look forward to our continued collaborations and friendship. José, thank you for your constant feedback and encouragement over the years that have immensely helped in improving the quality of this thesis. Thanks for your prompt and detailed reviews on all my publications. Chapters 2 and 4 would definitely not have been possible without your ideas/suggestions during year 1 of the PhD and for that I am truly grateful.

Next, I would like to express my gratitude to my co-promotor and daily supervisor, Dr. Alex Ștefanov, without whom, this thesis would not have been possible. Alex, thanks for all your support through thick and thin over the years and also letting me work on a topic that was rather alien to me (at that time). Although we may have different opinions on some topics, your never-say-die attitude, hard work, and attention to detail have shaped my scientific and professional growth. Also, getting to collaborate with industry and work on the CRoF was special that not many other PhDs get to experience. Furthermore, your vision for teamwork and not to work in individual "PhD silos" was a game changer. Thank you for everything.

I would also like to thank my doctoral examination committee for their time and efforts in reviewing my dissertation and providing crucial feedback that helped to greatly improve my thesis. I am also extremely thankful to have worked on the ERIGrid 2 project with an amazing consortium. Many thanks to Thomas and Elisabeth for their industrious project coordination and management that made my PhD life that bit easier. I would like to also thank all partners I worked with, especially JRA 2, 3, and 4 colleagues. I was really pleased with our collaborations and eventual outcomes. Hopefully, the RI-Energize proposal sees the light of day in some form or the other.

Thanks to the entirety of Alex's team who were an integral part of the PhD journey. I do miss our legendary morning meetings, but more so our group dinners. Firstly to

Alfan and Yigu who were there from the beginning. I am glad about our professional relationships transcending into personal ones over the years. Trips to Indonesia and China are definitely on the cards!

A big shoutout to my office mates over the years, including Alfan, Nicola, Kutay, Mohamad, and Ali. Especially Alfan and Nicola for our many discussions on all topics from A-Z. Mohamad, I look forward to our continued collaborations and am curious about the outcomes of your thesis. In the neighbouring office, thanks to Ioannis, Himanshu, Yigu, Sho, (formerly) Sjors and more recently Syed. I enjoyed all our lunch breaks and ensuing conversations. I also enjoyed my talks with Sho and May. Thanks to all and good luck with all your theses.

I would also like to thank all staff members of the IPEG group for their support and encouragement over the years. In particular, I am grateful to Dr. Milos Cvetkovic for supervising my master thesis that gave me the confidence to continue with a PhD. Thanks Milos for that! Next, the entire ESE support staff – including Ellen (formerly), Carla, Sharmila, Brenda, and Marieke. Special thanks to Carla for having 25 hours in a day to arrange all our requests and her continued support. This work would definitely not have been possible without the technical support staff, i.e., Remko and Simona. Remko, I truly enjoyed all our many conversations and coffee breaks since day 1 when you started at IEPG. Thanks also for humoring me with my broken Dutch. *Hartelijk dank voor het verbeteren van mijn Nederlands, ik ben er altijd dankbaar voor.* Your relentless support and enthusiasm meant a lot. I look forward to our continued friendship. Simona, thanks for helping us all improve in code reproducibility and documentation. I also enjoyed our many discussions about food and culture.

Many thanks also to Shivani and Carlos from team veggie tiffin for keeping me well-fed over the years. I never truly missed the comforts of home-cooked food, thanks to you! I would also like to thank Rishabh for his friendship and mentoring since the days of my master's and all the friends/colleagues from ESE and TUD I have had the pleasure of studying together and socializing with.

This thesis would definitely not have been possible without the support of my family – Amma and Appa, I am indebted to you for your unwavering support throughout this journey and hopefully have done you proud. Last, but not least, I am eternally thankful to my partner, Aishwarya for her continued support and encouragement that helped me cross the finish line. I look forward to our lifetime of adventures together!

Vetri  
Delft, 2025

# List of Publications

 Included in this thesis.

## Journal Articles

1.  **V. Rajkumar**, A. Ştefanov, J. L. Rueda Torres and P. Palensky, “Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks,” in *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 8807-8817, June 2024, doi:10.1109/TII.2024.3372024.
2.  **V. Rajkumar**, A. Ştefanov, A. Presekal, P. Palensky and J. L. Rueda. Torres, “Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures,” in *IEEE Access*, vol. 11, pp. 103154-103176, 2023, doi: 10.1109/ACCESS.2023.3317695.
3. A. Srivastava et al., “Digital Twins Serving Cybersecurity: More Than a Model: Cybersecurity as a Future Benefit of Digital Twins 2,” in *IEEE Power and Energy Magazine*, vol. 22, no. 1, pp. 61-71, Jan.-Feb. 2024, doi: 10.1109/MPE.2023.3325196.
4.  **V. Rajkumar**, M. Radwan, A. Ştefanov, and P. Palensky, “Preventive Islanding using Physics-Informed Graph Convolutional Networks for Cyber Resilience,” in *IEEE Transactions on Industrial Informatics* (under review).

## Conference Papers

5. A. Abedi, **V. Rajkumar**, A. Ştefanov and P. Palensky, “Towards Real-Time Distinction of Power System Faults and Cyber Attacks,” in *Proc. 2023 IEEE Power & Energy Society General Meeting (PESGM)*, Orlando, FL, USA, 2023, pp. 1-5, doi: 10.1109/PESGM52003.2023.10253241.
6. **V. Rajkumar** et al., “A Blueprint for Cyber Security of Brownfield Substations in Power Systems using IEC 62443” in *Proc. CIGRE Paris Session 2022*, Paris, France, 2022, pp. 1-12.
7. **V. Rajkumar** et al., “Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations,” in *Proc. CIRED 2021 - International Conference and Exhibition on Electricity Distribution*, Online Conference, Geneva, Switzerland, 2021, pp. 3092-3096, doi: 10.1049/icp.2021.2146.
8.  **V. Rajkumar**, et al., “Cyber Attacks on Power System Automation and Protection and Impact Analysis,” in *Proc. 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020, pp. 247-254, doi: 10.1109/ISGT-Europe47291.2020.9248840.

9.  **V. Rajkumar**, et al., “Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis,” in *Proc. 2020 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Sydney, NSW, Australia, 2020, pp. 1-6, doi: 10.1109/MSCPES49613.2020.9133698.

## Collaborative Publications

10. A. Presekal et al., Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems, in *IEEE Access*, vol. 12, pp. 177746-177771, 2024, doi: 10.1109/ACCESS.2024.3507386
11. A. Presekal et al., Cyber Security of HVDC Systems: A Review of Cyber Threats, Defense, and Testbeds, in *IEEE Access*, vol. 12, pp. 165756-165773, 2024, doi: 10.1109/ACCESS.2024.3490605.
12. S. Hashemi, M. Panteli, **V. Rajkumar** and A. Ştefanov, “Operational Mitigation of Cyberattack-Induced Cascading Failures in Power Systems,” in *Proc. 2024 International Conference on Smart Energy Systems and Technologies (SEST)*, Torino, Italy, 2024, pp. 1-6, doi: 10.1109/SEST61601.2024.10694287.
13. G. Silano et al., “Integrating Power-to-Heat Services in Geographically Distributed Multi-Energy Systems: A Case Study from the ERIGrid 2.0 Project, in *Proc. 2024 Open Source Modelling and Simulation of Energy Systems (OSMES)*, Vienna, Austria, 2024, pp. 1-6, doi: 10.1109/OSMES62085.2024.10668976.
14. I. Semertzis, H. Goyel, **V. Rajkumar**, A. Presekal, A. Ştefanov and P. Palensky, “Towards Real-Time Distinction of Power System Faults and Cyber Attacks on Digital Substations Using Cyber-Physical Event Correlation,” in *Proc. 2024 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Hong Kong, China, 2024, pp. 1-6, doi: 10.1109/MSCPES62135.2024.10542753.
15. **V. Rajkumar** et al., “Laboratory Middleware for the Cyber-Physical Integration of Energy Research Infrastructures,” in *Proc. 2024 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Hong Kong, China, 2024, pp. 1-5, doi: 10.1109/MSCPES62135.2024.10542755.
16. O. Gehrke et al., “Towards Automation of Configuration Management for Multi-Research Infrastructure Experiments,” in *Proc. 2023 Asia Meeting on Environment and Electrical Engineering (EEE-AM)*, Hanoi, Vietnam, 2023, pp. 1-6, doi: 10.1109/EEE-AM58328.2023.10490311.
17. A. Presekal, A. Ştefanov, **V. Rajkumar** and P. Palensky, “Cyber Forensic Analysis for Operational Technology Using Graph-Based Deep Learning,” in *Proc. 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Glasgow, United Kingdom, 2023, pp. 1-7, doi: 10.1109/SmartGridComm57358.2023.10333922.

18. A. Presekal, A. Ştefanov, **V. Rajkumar** and P. Palensky, “Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning,” in *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 4007-4020, September 2023, doi: 10.1109/TSG.2023.3237011.
19. L. Barbierato et al., “Exploring Stability and Accuracy Limits of Distributed Real-Time Power System Simulations via System-of-Systems Co-simulation,” in *IEEE Systems Journal*, vol. 17, no. 2, pp. 3354-3365, June 2023, doi: 10.1109/JSYST.2022.3230092.
20. L. Barbierato et al., “Stability and Accuracy Analysis of a Distributed Digital Real-Time Co-simulation Infrastructure,” in *IEEE Transactions on Industry Applications*, vol. 58, no. 3, pp. 3193-3204, May-June 2022, doi: 10.1109/TIA.2022.3155459.
21. I. Semertzis, **V. Rajkumar**, A. Ştefanov, F. Fransen and P. Palensky, “Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs,” in *Proc. 2022 Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Milan, Italy, 2022, pp. 1-6, doi: 10.1109/MSCPES55116.2022.9770140.

## Book Chapters

22. A. Presekal, A. Ştefanov, **V. Rajkumar** and P. Palensky, Cyber Attacks on Power Systems, in *Smart Cyber-Physical Power Systems: Challenges and Solutions*, Wiley-IEEE Press, In Press, Jan 2025.
23. A. Presekal, A. Ştefanov, **V. Rajkumar** and P. Palensky, Anomaly Detection and Mitigation in Cyber-Physical Power Systems based on Hybrid Deep Learning and Attack Graphs, in *Smart Cyber-Physical Power Systems: Challenges and Solutions*, Wiley-IEEE Press, In Press, Jan 2025.



# 1

## Introduction

*The increased digitalization of the power grid and transition to cyber-physical power systems raise serious concerns about cyber security and secure operation of the power system. It is now well recognized that information and communication technologies are vulnerable to cyber attacks. Thereby, electrical power grids as critical infrastructures are susceptible to cyber attacks as well. Malicious cyber attacks on power grid infrastructure can detrimentally affect power system operation and stability. In the worst-case, it can trigger cascading failures across the system, leading to a blackout. A coordinated cyber attack across multiple locations can collapse the entire interconnected power grid of nations, or even continents. This is a real modern-day threat, as seen during the cyber attacks on the Ukrainian power grid in 2015, 2016, and 2022. Therefore, power grid resilience and cyber security are now recognized challenges for power system operation and security of electricity supply. The gist of this entire thesis can be summarized as follows. “Analyze and demonstrate how cyber attacks on power grids may cause and accelerate cascading failures. Based on this analysis, develop suitable proactive defense measures to contain the spread of cascading failures.” Consequently, this is the core research focus of the thesis and is subsequently explained in the rest of this chapter.*

This chapter outlines the background and urgency of the research topic and this thesis, followed by the key research questions and scientific contributions.

## 1.1 Background and Motivation

The energy transition and a shift towards a more sustainable future is being driven by three key factors: decarbonization, decentralization, and **digitalization**. The integration of digital technologies is an important element for the future electrical power system. The integration of digital services in the OT domain has given rise to Industry 4.0 and increased Industrial Internet of Things (IIoT) presence in power grids. This has revolutionized power grid operations, enhancing efficiency and monitoring capabilities. However, this digital transformation has also introduced significant cyber vulnerabilities, exacerbating the risks associated with the convergence of Information and Communication Technology (ICT) and OT environments. As a result, cyber attacks on power grids have emerged as a sophisticated modern-day threat with wide-ranging ramifications. Such scenarios are no longer fictitious, as demonstrated by the cyber attacks conducted on the power grid in Ukraine in 2015, 2016, and 2022 [1, 2]. These incidents highlight the urgent need for robust cybersecurity measures to safeguard critical infrastructures such as power grids. Hence, this thesis aims to investigate the complex interplay between and impact of cyber threats on power system dynamics. The primary objective is to analyze and develop advanced strategies that bolster power grid cyber resilience, thereby ensuring the security of supply amidst cyber attacks.

The societal implications of this research are critical. Power grids are foundational to modern societies, underpinning essential services such as healthcare, transportation, and communications. Enhancing their resilience against cyber threats is not merely a technical challenge but a societal necessity. This research contributes to the overarching goal of ensuring a cyber resilient power system which is vital for societal well-being and economic stability. In summary, this section establishes the foundation for the subsequent detailed analysis and solutions, underscoring the urgency and significance of the research in addressing contemporary cyber threats to power grids.

## 1.2 Power Grid Digitalization and Cyber Security

Increasing power grid digitalization has resulted in the convergence between ICT and OT systems. While offering greater monitoring and control capabilities, this has brought forth serious cyber security concerns. Cyber attacks on power grids are high impact, low frequency events with a wide range of consequences. These could include, but are not limited to, equipment damages, loss of load, and power system instability. In the worst case, sophisticated cyber attacks may also cause system-wide cascading failures, leading to a blackout.

Figure 1.1 presents a brief timeline of cyber security incidents involving power systems in the past 5–6 years. It is evident that there is an ever increasing threat of cyber attacks on power systems. The attack in Ukraine in 2015 caused intermittent power outages, affecting more than 225,000 people. In 2016, a sophisticated malware was used that led to a disruption in the distribution network. This resulted in the loss of over 200 MW of load and a power outage. Meanwhile, on March 9, 2020, it was reported that the IT net-

work of European Network of Transmission System Operators for Electricity (ENTSO-E) was compromised in a cyber intrusion. More recently, on October 12, 2020, Mumbai, a major Indian metropolis was affected by a power outage lasting over 12 hours. A later study revealed that the outage was related to ‘RedEcho’, an active hacker group. The attackers used sophisticated malware to target a regional control centre, in a campaign lasting over 6 months. Later, in 2022, an IT system related cyber attack affected 11 GW of German wind farms. Around the same time, Ukraine was targeted again by the Industroyer 2 malware, exploiting microSupervisory Control and Data Acquisition (SCADA) vulnerabilities. Thus, cyber security of power systems has emerged as a dynamic and critical area of research [3, 4].

Given this scenario, there is a pressing need to understand if and how cyber attacks can lead to cascading failures and blackouts in power systems. By conducting a thorough analysis of past blackouts, critical root causes of cascading failures can be identified, with a focus on cyber-physical aspects. This can help to develop effective strategies for mitigating the impact of cyber attacks and minimizing the likelihood of widespread power outages. Furthermore, by understanding the root causes of blackouts, appropriate measures can be taken at an early stage to avoid cascading failures and maintain the resilience of power systems in the face of cyber threats.

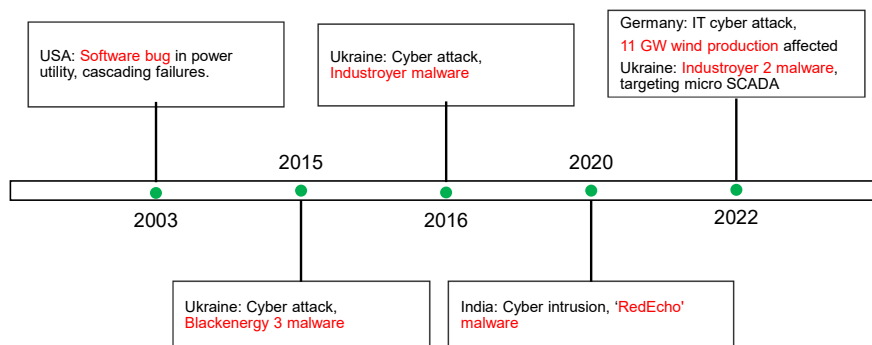


Figure 1.1: Timeline of power system related cyber security incidents from 2003 to 2022.

## 1.3 State-of-the-Art

In this section, we discuss the existing literature on cascading failure analysis and cyber security for power systems. Based on this analysis, research gaps to be addressed are outlined in the subsequent section.

### 1.3.1 Cascading Failure Analysis Methods

The preliminary step to analyze the impact of cyber attacks on power grids is to study the cascading failure mechanism that is predominant across all major recorded power system blackouts. Methods to study and analyze blackouts are not new and have been investigated quite extensively in the literature. A major part of existing work has focused on

analysis of cascading failures and blackouts from a steady-state perspective. Typically, these include quasi-steady state DC power flow models that can capture overloading conditions. Similarly, AC power flow models have also been proposed and extensively investigated. However, a major drawback of such methods is the inability to study non-linear mechanisms, such as loss of synchronism and voltage collapse that have been observed in real-world cascading events. Other techniques include statistical methods based on historical data to describe the behaviour of cascading failures. While offering general analytical insights, such methods do not provide detailed information that is obtainable from simulations. Another class of models are topological models that rely on network/graph theory to describe the mechanism of cascading failures. However, without consideration of actual power system physics and power flows, such models cannot provide accurate in-depth system specific insights.

Based on Table 1.1, the following can be summarized. Limited work has been carried out in employing dynamic RMS-based power system models to study cascading failures direction. This is highly important as it is critical to study non-linear dynamic mechanisms in detail. Further, in the advanced stages of any blackout, dynamic phenomena, i.e., frequency, voltage and transient stability dominate, which cannot be completely captured by existing steady-state methods. Hence, a switch to dynamic time-domain simulations is needed that can effectively capture cascading failures and associated dynamic phenomena. This is particularly relevant to this research which considers the potential impact of cyber attacks on power system dynamics.

Table 1.1: Summary of cascading failure models and analysis methods.

| Type of Model/Analysis                      | Year | Source |
|---------------------------------------------|------|--------|
| Steady State: CASCADE Model                 | 2007 | [5]    |
| Steady State: ORNL-PSerc-Alaska (OPA) model | 2009 | [6]    |
| Graph Theory                                | 2010 | [7]    |
| Steady State: DC power flow                 | 2012 | [8]    |
| Review of existing methodologies            | 2013 | [9]    |
| Quasi Dynamic                               | 2016 | [10]   |
| Dynamic Model: COSMIC                       | 2016 | [11]   |
| Steady state with dynamic models            | 2021 | [12]   |
| Acceleration of cascading outages           | 2022 | [13]   |

### 1.3.2 Cyber Security for Power Grids

Similar to the above section, a detailed literature study into cyber security for power grids reveals the following. A significant portion of previous work has focused on development of experimental testbeds and analysing the impact of specific cyber attacks using them. Only limited work has been conducted in developing (semi) analytical methods to analyze cyber attacks and their impact. Furthermore, another identified gap is the limited work on the investigation of potential large-scale impact of cyber attacks on power grids. Thus,

more detailed studies on impact of cyber attacks on power grid stability and cascading failures are needed. This is better summarized in Table 1.2.

Table 1.2: Summary of cyber attacks and their impacts on power systems.

| Type of Attack and Impact                                       | Year | Source |
|-----------------------------------------------------------------|------|--------|
| Cyber security of power system                                  | 2010 | [14]   |
| Network delays on SVC: impact on transient stability            | 2014 | [15]   |
| Multi switch attacks for cascading failures                     | 2014 | [16]   |
| Communication line outage, DoS, and MiTM                        | 2015 | [17]   |
| IEC 61850 GOOSE                                                 | 2016 | [18]   |
| Smart grid cyber security overview                              | 2018 | [19]   |
| Data integrity and manipulation attacks on multiple substations | 2018 | [20]   |
| Aurora attack; Microgrid generator switching compromised        | 2019 | [21]   |
| Cyber attacks on power system protection                        | 2020 | [22]   |

## 1.4 Research Gaps

The literature survey from the previous section leads to the following research gaps which are addressed in this thesis:

- Limited previous work exists on investigation of large-scale impact of cyber attacks on power grids. This area of research has gained widespread interest in the wake of Ukraine cyber attacks, post 2015 and 2016. Hence, this is an ever-evolving research topic.
- There is a lack of detailed quantitative analysis of cyber attack impact on power grid stability. This begs the question, “*can cyber attacks induce cascading failures and lead to a blackout?*”
- Existing work in this area has focused on analysis through numerical co-simulations and testbeds. Therefore, analytical approaches and methods are needed to conclusively show that cyber attacks can indeed cause cyber attacks and lead up to the point of no return. As a result, they can also accelerate cascading failures.
- Limited dynamic models and analyses to study cascading failures. This is highly important as it is critical to study non-linear dynamic mechanisms in detail. Furthermore, in the advanced stages of any blackout, dynamic phenomena, i.e., frequency, voltage and transient stability dominate, which cannot be completely captured by existing steady-state methods.
- With increased power grid digitalization, the threat of cyber attacks is only bound to increase. Existing preventative measures are focused on mitigation of root causes for physical disturbances. However, cyber attacks are fast and dynamic events. Thus, there is a need for preventive or automated techniques to defend power grids in the face of cyber induced cascading failures.

## 1.5 Overall Thesis Objective and Research Questions

Based on the state-of-the-art analysis and identified research gaps, the gist of this entire thesis can be summarized as follows, ***“analyze and demonstrate how cyber attacks on power grids may cause and accelerate cascading failures. Based on this analysis, develop suitable proactive defense measures to contain the spread of cascading failures.”*** Consequently, the key research questions associated with this thesis are as follows:

### RQ 1 Can cyber attacks cause and accelerate cascading failures?

This research question raises the following pertinent sub questions:

- 1.1 How to show qualitatively and quantitatively that cyber attacks can cause cascading failures in power systems?
- 1.2 How to prove semi-analytically that cyber attacks can cause cascading failures in power systems?
- 1.3 How to prove that cyber attacks can accelerate the cascading failure mechanism compared to physical disturbances?

### RQ 2 How defend against cascading failures caused by cyber attacks?

The associated sub questions are as follows:

- 2.1 How to secure IEC 61850 GOOSE messages to mitigate cyber attacks on digital substations?
- 2.2 How to mitigate the impact of cyber attacks using proactive approaches to contain the spread of cascading failures in power systems?

## 1.6 Methods/Approaches

In this section, the proposed methods to address the aforementioned research questions and their associated justifications are discussed as follows.

### RQ 1.1: How to show qualitatively and quantitatively that cyber attacks can cause cascading failures in power systems?

This research question can be broken down into two sub-questions – covering the qualitative and quantitative analysis, respectively. To address the former, as described in the following Chapter 2, we perform a systematic survey of major historic blackouts caused by physical disturbances to examine and understand the cascading failure mechanism. Subsequently, we identify critical cyber-physical factors that can activate and influence it. Based on this, we hypothesize and qualitatively connect the dots to show how cyber attacks on power grids may cause cascading failures and a blackout.

To address the latter, i.e., to show quantitatively that cyber attacks can cause cascading failures in power systems, numerical simulations and Hardware-in-the-Loop (HIL)-based experiments are undertaken. A modified version of IEEE-39 bus test system is developed, consisting of multiple, coordinated protection schemes to simulate cascading failures. This is connected to a dedicated OT network emulator to perform numerical cyber-physical co-simulations and assess impact of cyber attacks on power system dynamics. Furthermore, cyber attack exploits, impact on power system dynamics and cascading failures are experimentally verified through a dedicated HIL setup. This closely resembles real-world conditions within a digital substation, including Intelligent Electronic Devices (IEDs) and protection schemes.

**RQs 1.2 and 1.3: How to prove semi-analytically that cyber attacks can cause and accelerate cascading failures in power systems?**

A detailed and purely analytical study of the dynamic power grid model and capturing its interaction with discrete cyber actions is a challenging task. Hence, this thesis utilizes numerical simulations using the aforementioned dynamic power grid model with multiple power system protection schemes to conduct data-driven analysis. One of the major objectives of this research is to characterize the point of no return caused by cyber attacks. Parameters involving power system dynamics obtained from time-domain simulations are typically non-linear and non-stationary in nature. Analysis of this simulation data provides detailed insights into the dynamics of the system such as stability margins and mode changes. To do so, time-frequency analysis can be performed. A popular method reported in literature to achieve this is the Hilbert-Huang Transform (HHT). As reported in [23], this approach, “retains the time-domain information of the signal without compromising on its frequency-domain analysis.” Hence, this technique can track temporal variations in the frequency and amplitude of an input time-series signal. As a result, interesting properties of system behaviour can be explored. This motivates the application of this technique on power system simulation data to ascertain semi-analytically how cyber attacks can cause cascading outages, as further described in Chapter 4.

To address the latter question, it is first important to understand the cascading failure mechanism. A complete cascading failure can take anywhere between minutes to hours, comprising of both ‘slow’ processes and ‘fast’ dynamic events, as better described in Chapter 2. Thus, any cascading failure can be split up into a slow phase and fast phase. However, there is no accepted standardization for this splitting or the average time in each phase, as discussed in [12]. Furthermore, as reported in [11, 24] large-scale blackouts typically exhibit an exponential probability distribution in terms of size in the fast phase. Hence, numerical simulation comparisons between cyber and physical disturbances are conducted in Chapter 4 to demonstrate how due to targeted cyber attacks, the entire cascading failure mechanism can be accelerated leading to a quicker shift to the fast phase.

**RQ 2.1: How to secure IEC 61850 GOOSE messages to mitigate cyber attacks on digital substations?**

To ensure Generic Object Oriented Substation Event (GOOSE) message integrity and authenticity, a custom hardware setup is developed as described in Chapter 3. Such an architecture is referred to as bump-in-the-wire without any major changes needed to the network settings. A dedicated device such as a Raspberry Pi calculates the MAC value and appends it to the GOOSE message that is then sent to the subscriber. The subscriber recalculates a new value of the MAC code based on the received GOOSE message and shared private key. This value is then compared to the one appended in the received GOOSE message. If it matches, it means the message is authentic and originates from the correct IED and has not been tampered with. If not, there is some issue. Thus, the authenticity of the sent messages and identity of the associated publisher is clearly verified. As a result, spoofing and replay attacks are mitigated. Furthermore, detailed statistical performance analysis of the implementation is performed to show that the end-to-end latency HMAC process is well within 3-4 ms.

**RQ 2.2: How to mitigate the impact of cyber attacks using proactive approaches to contain the spread of cascading failures in power systems?**

Cyber-physical power systems are vulnerable to cyber attacks that may lead to cascading failures and power outages. A promising solution to tackle this emerging issue is the concept of preventive/proactive controlled islanding before the attack actually occurs, based on early detection of cyber attacks. Hence, in this thesis, a novel physics-informed graph convolution network is used to perform preventive controlled islanding. The usage of physics-informed Graph Convolutional Network (GCN) is scientifically motivated by its ability to integrate power system physics into neural network loss functions, ensuring that the resulting islands are self-sufficient and stable in terms of voltage and frequency. By representing power systems as graphs, GCN can effectively capture both local and global dependencies, making them well-suited for modeling the spatial as well as temporal dynamics of power systems. Moreover, incorporating physical laws into the model increases its interpretability. Hence, this work paves the way towards cyber-physical system resilience of power systems against cyber induced cascading failures.

### Assumptions

The list of key assumptions, based on the above sections of this thesis are as follows.

- **No remedial actions:** It is assumed that during the analysis and simulation of cascading failures, no remedial actions are taken by system operators. This allows for a clear observation of the natural progression of failures without intervention, providing a baseline for understanding the impact of cyber attacks.
- **Fast-phase of cascade:** The focus of this thesis is primarily on the fast-phase of the cascading failure process, wherein dynamic events occur rapidly. This phase is critical for understanding how cyber attacks can accelerate the cascading failure process and lead to quicker system collapses.
- **IDS Input Available:** It is assumed that intrusion detection system (IDS) data is available and reliable. This data is crucial for early detection of cyber attacks, enabling

proactive measures such as controlled islanding to mitigate potential cascading failures.

- **Cyber attack scenarios:** The cyber attack scenarios used in the simulations are representative of real-world threats. This includes assumptions about the attacker's capabilities, targets, and methods.
- **Stable initial conditions:** The power system is assumed to be in a stable initial state before the introduction of any cyber attacks. This allows for a clear attribution of any subsequent instabilities or failures to the cyber attacks themselves.
- **No external disturbances:** During the simulation period, it is assumed that there are no other external disturbances that could independently cause cascading failures. This isolates the effects of cyber attacks for clearer analyses.
- **Protection schemes:** The protection schemes in the power system are assumed to be functioning as designed. This ensures that the simulations accurately reflect the system's response to cyber attacks. No equipment failures or malfunctions are considered.

## 1.7 Scientific Contributions

Based on the above research questions, the key contributions and outcomes of this thesis are summarized as follows:

### Contribution 1

Proved qualitatively and quantitatively how cyber attacks can cause power system cascading failures. This is based on a particular case study that is also generally applicable to any other power system with similar dynamics.

### Contribution 2

Developed a method to define, identify, and numerically quantify the point of no return with experimental results to validate how cyber attacks can accelerate the cascading failure mechanism. This is compared to historical blackout events to highlight the increased speed and impact of cyber induced cascading failures.

### Contribution 3

Demonstrated the implementation of IEC 62351-6 compliant HMAC to secure GOOSE messages with respect to real-time requirements for power system protection and mitigate replay and spoofing cyber attacks in digital substations.

### 🏆 Contribution 4

Developed an AI-based method for preventive controlled islanding to minimize and contain the impact of cyber induced cascading failures. This provides system operators with decision making recommendations to curtail the spread of power system cascading failures caused by cyber attacks.

## 1.8 Thesis Outline

The structure and outline of the rest of this thesis, based on the research questions is depicted in Figure 1.2.

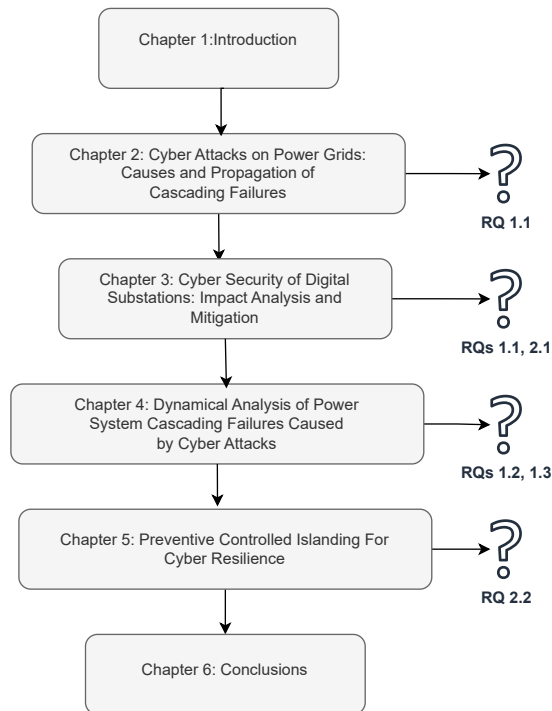


Figure 1.2: Thesis outline and relation to research questions.

Chapter 1 introduces the thesis in context with a specific focus on power grid digitalization and cyber security. As power systems undergo a digital transformation, the risk of cyber threats should not be taken lightly. Such cyber threats pose potentially serious dangers to the stability and reliability of power systems. Furthermore, this chapter also elucidates the critical research objectives and scientific contributions, thereby highlighting the urgent need for robust cyber security measures. This chapter lays the foundation

for a compelling exploration of the complex interplay between power grid digitalization and cyber security, digital substations, cascading failures, and resilience. This underscores the imperative of this research in safeguarding our energy infrastructure against emerging cyber threats.

Chapter 2 delves into the qualitative analysis of how cyber attack may cause cyber attacks. The chapter explores how cyber attacks could trigger cascading failures in power systems. Traditionally, cascading failures result from rare, simultaneous physical disturbances, but increased digitalization makes grids vulnerable to cyber threats. Given the lack of real-world cyber attack data, this chapter examines the potential for cyber attacks to initiate and accelerate cascading failures by reviewing major blackouts caused by physical disturbances.

Chapter 3 examines cyber security risks in digital substations, focusing on the vulnerabilities in the IEC 61850 standard. Cyber attacks can exploit these vulnerabilities by injecting spoofed messages, thereby disrupting or tripping protective relays and potentially disconnecting generation and transmission lines. Finally, mitigation measures, specifically hash-based message authentication codes from the IEC 62351-6 standard to counter these attack methods are implemented and analyzed.

Chapter 4 proves semi-analytically how cyber attacks can both initiate and accelerate cascading failures in power systems. Cascading failures, though rare, are caused by the occurrence of multiple low-probability events. The escalating threat of cyber attacks on power grids introduces the potential for large-scale cascading failures, culminating in blackouts. To address this challenge, this chapter introduces a novel data-driven method for the dynamic analysis of cyber-induced cascading failures. Through experimental validation, we illustrate how cyber attacks can significantly accelerate the cascading failure process compared to historically observed blackouts caused by physical disturbances.

Chapter 5 introduces a novel proactive AI-based preventive islanding solution to mitigate the impact of cyber attack-induced cascading failures. This innovative approach aims to contain and minimize the spread of cascading outages by implementing controlled islanding before the cyber event occurs, leveraging early-stage detection of cyber threats. The chapter proposes a novel physics-informed graph convolutional network that integrates power system physics into the neural network's loss function formulations. This integration ensures that the resulting islands are self-sufficient and stable in terms of voltage and frequency. Experimental simulations demonstrate the efficacy of the proposed method through significant reduction in the loss of load, up to 90% when a single substation is compromised and 62% in the case of multiple compromised substations. By advancing the concept of preventive controlled islanding, this research contributes substantially to enhancing the cyber resilience of power systems.

Chapter 6 provides a comprehensive summary of the major findings and conclusions derived from this thesis, underscoring their significance within the broader context of power grid cyber security. This chapter examines the implications of the research, highlighting how the proposed methodologies and insights contribute to enhancing the cyber resilience of power systems against cyber threats. Furthermore, the chapter identifies avenues for future research, emphasizing the need for continued innovation and interdisciplinary research to address emergent challenges in the field.



## 2

## Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures

*Cascading effects in the power grid involve an uncontrolled, successive failure of elements. The root cause of such failures is the combined occurrence of multiple, statistically rare events that may result in a blackout. With increasing digitalization, power systems are vulnerable to emergent cyber threats. Furthermore, such threats are not statistically limited and can simultaneously occur at multiple locations. In the absence of real-world attack information, however, it is imperative to investigate if and how cyber attacks can cause power system cascading failures. Hence, in this chapter we present a fundamental analysis of the connection between the cascading failure mechanism and cyber security. We hypothesize and demonstrate how cyber attacks on power grids may cause cascading failures and a blackout. To do so, we perform a systematic survey of major historic blackouts caused by physical disturbances, and examine the cascading failure mechanism. Subsequently, we identify critical cyber-physical factors that can activate and influence it. We then infer and discuss how cyber attack vectors can enable these factors to cause and accelerate cascading failures.*

## 2.1 Introduction

The electrical power grid is one of the most complex man-made systems, providing electricity worldwide. However, like any other large-scale system, it is prone to large-scale failures and catastrophes [25, 26]. This issue is exacerbated by the increasing interconnection of power grids across continents and countries. This in turn makes it vulnerable to failures with origins at different locations. Such failures can result in disruption of power supply, or failure to meet basic power quality requirements. Consequently, disruption of public services can occur, e.g., transportation, communications, domestic power supply, etc. Furthermore, these outages result in large penalties to system operators. Hence, it is of paramount importance to mitigate the effects of such failures and minimize damage caused [27].

### 2.1.1 Cascading Failures and Blackouts

The blackout state is defined by European Network of Transmission System Operators for Electricity (ENTSO-E) as, “*the interruption of electricity generation, transmission, distribution and consumption processes, when operation of the transmission system or a part thereof is terminated.*” The disastrous impacts of blackouts are well known, with severe technological and socioeconomic ramifications, affecting all spheres of societal functioning. It is seen that power outages are a persistent problem, caused by a multitude of reasons. Some of the most common reasons include, but are not limited to, extreme weather, high load demand, poor system planning, etc. Hence, a blackout is caused by a combination of multiple, mutually exclusive, low probability events. This brings into play the mechanism of cascading failures. A cascading failure is “the uncontrolled successive loss of system elements triggered by an incident at any location.”

This brings into play the mechanism of cascading failures. A cascading failure is “the uncontrolled successive loss of system elements triggered by an incident at any location.” Most blackouts are initiated by some major disturbances in the power grid, leading to a propagation of cascading failures across the entire system [13, 28, 29]. The number of affected users, country of origin, and year of occurrence of some major global blackouts in the time period 2003–2022 is shown in Figure 2.1. As can be seen from the figure, in the past 10 years, several significant blackouts have occurred worldwide. In 2003, USA and Canada experienced a 48-hour blackout affecting 50 million people, while Italy suffered a 12-hour blackout affecting 60 million people. In 2006, the ENTSO-E region had a 3-hour blackout impacting 15 million people. The largest blackout, in terms of affected consumers occurred in India in 2012 during severe 15-hour blackout, affecting a staggering 620 million people. Other notable blackouts include Turkey in 2015 for about 8 hours, affecting 70 million and Pakistan in 2021 (9 hours, 200 million people affected).

The most common reasons for these blackouts were adverse weather conditions, highly stressed systems or a combination of thereof. Increasing integration of renewable energy sources and the rapid digitalization of the power system has significant implications on power system cascading failures. This combination creates a complex interplay between physical and cyber-physical aspects of the power system. The reliance on interconnected and interdependent systems may amplify the potential impact of cascading failures. A localized disturbance or failure in one part of the system can propagate through digital communication networks and physical components, leading to widespread outages and

disruptions. This interplay between the cyber and physical worlds is subsequently discussed at length in the rest of this chapter.

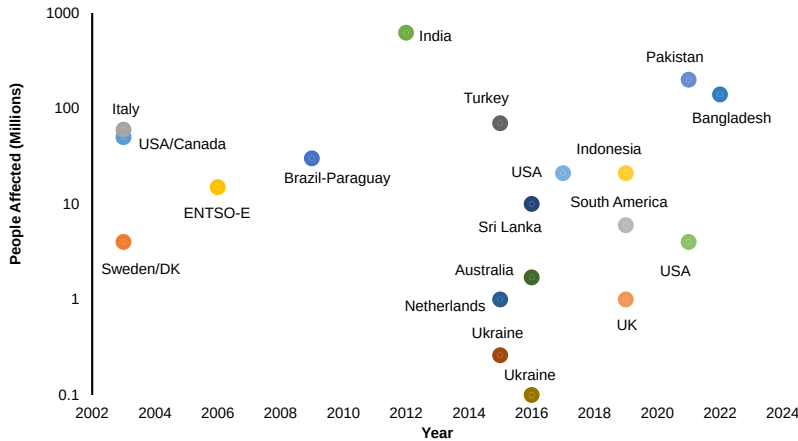


Figure 2.1: Major global power system blackouts between 2003–2022 and their societal impact.

### 2.1.2 Modelling of Cascading Failures

Various modelling approaches for understanding the mechanisms behind cascading failures in power grids are discussed in [30]. The authors investigated the impact of different factors such as node connectivity, load distribution, and protection schemes on the likelihood of cascading failures. In [31], the authors analyzed the vulnerability of power grids to cascading failures under different scenarios, including random failures and targeted attacks. While the aforementioned works provide valuable insights into cascading failures in power grids, they do not address the cyber-physical factors that can influence such failures. In [32], the authors discuss the resilience of cyber-physical systems against natural hazards and cyber attacks. They consider human and societal factors that can affect system resilience, such as organizational structure and communication patterns. The impact of cyber attacks on the power system, however, is not discussed in detail, nor are the critical cyber-physical factors that can influence the cascading failure mechanism. Overall, further research is needed to fully understand the complex interplay between cyber and physical components in power grids and their impact on system stability. Hence, our work seeks to address this gap.

### 2.1.3 Cyber Security of Power Grids

Review of cyber security for power systems is well reported in the literature [33]. For example, in [34], the authors provide a comprehensive review of cyber attacks and defence mechanisms for improving smart grid security. This work provides an overview of all the topics in this research domain, i.e., cyber security, modelling, interplay between cyber and physical layers in CPS, etc. Similarly, [35] discusses vulnerability assessment for cyber-physical power systems. More importantly, this work reviewed methods to assess

vulnerability and resilience and identified existing gaps. Meanwhile, cyber-physical security and cyber-physical attack scenarios are discussed in depth in [36]. All these works seek to provide a better understanding of vulnerabilities in cyber-physical systems and propose suitable resilience solutions. However, they miss connecting the cyber and physical worlds, i.e., how cyber threats can affect the power system cascading failure mechanism, which forms the focus this chapter.

### 2.1.4 Review of State-of-The-Art

Based on the current state-of-the-art literature review, five categories of interest were identified and a detailed comparison of reviews and surveys addressing these topics is provided in Table 2.1.

Table 2.1: Classification and comparison of state-of-the-art literature.  
Coverage: L–Low; M–Medium; H–High

| Ref. | CF Analysis | C-P Factors | Cyber Security | Cyber Attacks | Validation | Remarks                                                             |
|------|-------------|-------------|----------------|---------------|------------|---------------------------------------------------------------------|
| [37] | L           | M           | M              | L             | L          | Discussed vulnerability assessment and resilience aspects for CPPS. |
| [38] | L           | L           | H              | M             | L          | Proposed a privacy conserving framework for intrusion detection.    |
| [39] | L           | M           | H              | H             | L          | Comprehensive review of CPPS attack vectors and defense mechanisms. |
| [40] | L           | L           | M              | H             | L          | Explored methods to quantify resilience in CP power systems.        |
| [41] | L           | H           | H              | L             | L          | Advanced review on CPPS modelling and threat analysis.              |
| [33] | L           | L           | H              | H             | L          | Focused on CPS threats, attacks, and mitigation techniques.         |
| [42] | M           | L           | M              | L             | L          | Summary of CPS definition and metrics for quantification.           |
| [43] | H           | H           | L              | L             | L          | Comprehensive review of generalised cascading failure mechanism.    |
| [44] | L           | M           | H              | H             | L          | Thorough review of CPS modelling and cyber security                 |

1. **Cascading failure analysis:** encompasses studies and research related to the modelling and analysis of cascading failures within power systems. This includes identifying vulnerabilities and potential points of failure. This category is chosen as it is crucial for understanding the fundamental aspects of power system reliability and resilience, and focuses on the root causes of cascading failures.
2. **Cyber-physical factors:** research that delves into the interplay between cyber and physical layers in power systems. This category is chosen to understand how cyber attacks can propagate and impact the physical infrastructure. Such knowledge is essential for devising strategies to safeguard power systems from cyber threats that can lead to cascading failures.
3. **Cyber security of power grids:** concentrates on the various cyber security threats, protocols, and technologies that can affect the power grid.
4. **Cyber attacks:** focuses on the different methods and strategies that cyber attackers employ to target power systems, including malware, phishing, and Advanced Persistent Threats (APTs).

5. **Experimental validation:** This category deals with empirical studies and experiments aimed at validating the impact of cyber attacks on power system cascading failures and proposing suitable mitigation strategies

## 2.2 Review of Historical Blackouts

2

This section summarizes some major blackout events in the period 2003-2021. A summary of the sequence of events leading up to the blackout is provided, based on available literature. Through this summary, we aim to identify the critical factors that initiated the cascading failures, leading to the blackout. A detailed summary of multiple blackouts is provided in Table 2.2.

### 2.2.1 Italy, 2003

On September 28, 2003, the Italian power system experienced a major blackout. The outage affected an area housing around 60 million people. The triggering event began at 03:01:00 and proceeded up to 03:28:00. Power was restored after three hours in the North and later in the day in the rest of Italy. In total, approximately 6.4 GW of load was left unmet. This was deemed to be the largest blackout in the country's history, and one of the biggest within the EU [36]. The blackout was initiated by a fault originating in neighbouring Switzerland, triggering a chain of cascading events. This eventually resulted in the Italian power grid being cut off from the rest of Europe. The entire sequence of events can be summarized as follows. A tree flashover caused a 380 kV tie line trip in Switzerland near the Italian border, resulting in failed breaker controls and power transfer to Italy through neighbouring lines. Despite a 300 MW import reduction, a second tie line also tripped near the Swiss-Italian border due to poor operator response and inadequate power redistribution. Additional power was imported from France without prior planning. This overloading of tie-lines to France led to a drop in system frequency, triggering under-frequency relays, generator disconnections and a complete blackout. The major identified reasons were inadequate coordination, lack of real-time monitoring, reduced security margins, increased parallel flows, and angular and voltage instabilities, causing system collapse.

### 2.2.2 USA-Canada, 2003

On August 14, 2003, a blackout occurred in North America involving eight U.S. states and two Canadian provinces. Approximately 50 million people were affected and around 63 GW of load was lost or interrupted [45]. This equated to roughly 11% of the total load served in the Eastern Interconnection of the North American system. Over the course of the entire event, more than 400 transmission lines and 531 generating units at 261 power plants tripped. The blackout resulted from a combination of multiple unrelated events. Due to weather conditions and excess vegetation, flashovers took place on overhead transmission lines. A previously unknown and critical software bug, i.e., a race condition in the alarm system at the control room of the system operator, First Energy (FE) [4] led to inadequate situational awareness. This blindsided system operators who were unaware of actual ground conditions and the need to take remedial actions after the tripping of multiple transmission lines. This set off a chain of major cascading failures, culminating in one

of the largest blackouts in American history [45].

A brief summary of the sequence of events is as follows. A generator outage occurred due to over-excitation caused by high reactive power output from other generators Northern Ohio service area. Unrelated, multiple 345 kV transmission lines experienced flashovers and trips due to vegetation contact, despite not being overloaded. Lack of situational awareness caused by a software bug at FE resulted in no operational actions being taken, leading to cascading line trips and severe under voltage conditions. A critical transmission line tripped in Ohio, triggering cascading failures in other nearby transmission and tie-lines with similar settings. This sudden loss of major tie lines caused power transfer between the U.S. and Canada to reverse, resulting in a huge power flow of around 3700 MW from Canada to Michigan and Ohio. This unplanned exchange caused voltage collapse due to overloaded transmission lines, leading to cascading failures of other lines and generators, resulting in a blackout.

### **2.2.3 Europe, 2006**

The European transmission system experienced a major blackout on November 4, 2006, affecting around 15 million people. The origin of the events leading up to the blackout took place in Germany, but quickly spread throughout the continent. The main causes of the blackout were identified as the non-fulfilment of the N-1 criterion and insufficient coordination amongst Transmission System Operators (TSOs). The N-1 criterion was violated when appropriate security analysis and application of pre-defined remedial actions were not performed. In addition, the compliance with the criterion was evaluated by a TSO regardless of the situation in the neighbouring systems. Furthermore, results of security analysis between TSOs were not robust and wide enough. The crucial factors that influenced the blackout were limited range of actions for handling grid congestions, lack of coordination throughout the event and generator related issues.

### **2.2.4 India, 2012**

The largest blackout in terms of people affected, occurred in July 2012, in India [46]. Extremely hot weather conditions led to a very high system demand, placing tremendous stress on the power system. On 30 July 2012, around 02:00 local time, a 400 kV tie-line interconnecting the western and northern regions tripped, initiating a chain of events, culminating in a large-scale blackout. Successive line trips after the initial event led to a power imbalance of around 32 GW. This left around 300 million Indians in the dark. The socioeconomic ramifications were disastrous, affecting core sectors such as transport, healthcare, finance, etc. As per the post incident report, the root causes for the blackout were identified to be weaker transmission line corridors and protection malfunction. Other critical factors such as lack of coordination for outages, frequency control and islanding methods aggravated the effects [47].

### **2.2.5 Turkey, 2015**

The Turkish power system experienced a blackout on March 31, 2015 that lasted for over 8 hours. The blackout was initiated by a major tie-line trip due to overload. This disconnected the eastern and western regions. Subsequently, other lines became overloaded and tripped in succession (violation of N-1 criterion). Thus, the eastern and western parts were

separated resulting in a major power mismatch. The eastern region had excess supply, resulting in an over frequency condition leading to protection trips. Conversely, the western part suffered from under frequency, leading to load shedding. However, power plants could not operate at reduced frequencies for extended durations, leading to a blackout. The most critical factors in this event were found to be the lack of real-time monitoring and contingency preparedness. Furthermore, a lack of awareness about the effects of angular stability, distance relay settings, and grid code compliance compounded the issue.

### 2.2.6 United Kingdom, 2019

On August 9, 2019, a major power outage in the UK affected over 1 million consumers' electricity supply. Several inter- dependent services were disrupted due to the outage. Rail services were severely affected, causing major socioeconomic disruptions. The event was found to be caused by a lightning strike prior to the blackout that triggered a process known as vector shift protection. This automatically reduced power output by 150 MW to ease the strain on the network. These outages also triggered a collapse in the frequency, which plummeted to 48.8 Hz during the blackout. This caused load shedding schemes to activate and disconnect about 350 MW of power from grid, allowing the frequency to recover. This unintentional load shedding however, had an adverse impact on electricity reliant critical services such as railways and hospitals.

### 2.2.7 Pakistan, 2021

The entire nation of Pakistan was plunged into darkness in the wee hours of January 9, 2021. The blackout was caused by electrical fault in southern Pakistan at 23:41 hrs. local time, which prompted a series of cascading outages. The total restoration process took around 20-22 hours in some areas. The post incident analysis report mentions a permanent bolted earth fault and unstable power swings as the root causes. Furthermore, lack of operator experience and negligence also played a key role.

### 2.2.8 Summary

Based on the above incidents, the anatomy of a power system blackout can be summarized as follows:

1. **Preconditions:** refer to the underlying conditions or vulnerabilities in the power system that may exist prior to a blackout. These can include factors like inadequate infrastructure, insufficient maintenance, or operational limitations.
2. **Triggers:** events or factors that initiate the blackout. They can be external events such as severe weather conditions, natural disasters, equipment failures, or human errors. Triggers can also be internal factors like system overloads or voltage instability.
3. **Emergency condition and remedial actions:** once the triggers occur, the power system enters an emergency condition. At this stage, various remedial actions need to be undertaken to stabilise the system and prevent a complete blackout. These actions may include load shedding, generation adjustments, or rerouting of power flows.

- 4. **Other triggers:** apart from the initial triggers, there can be additional factors that contribute to the escalation of the blackout. These can include secondary equipment failures, lack of contingency plans, or ineffective actions by the system operator.
- 5. **Slow and fast cascading failures:** cascading failures refer to the progressive and interconnected failures that occur in a power system. They can be categorised as slow or fast depending on the speed at which they propagate. Slow cascading failures are characterised by a gradual deterioration of the power system, where the failure of one component leads to increased stress on others, eventually resulting in system-wide disruptions. Fast cascading failures, on the other hand, exhibit a rapid and simultaneous collapse of multiple components, leading to a sudden and severe blackout. Sometime between these two phases, the Point of No Return (PNR) is reached. This denotes an inflexion point between the stages and results in a blackout, i.e., loss of power supply to a significant portion or the entire power system.

In summary, all electrical power grids are designed to comply with the *N-1* criterion, i.e., a single component/element failure does not result in the collapse of the entire system. Nonetheless, a unique combination of failures can induce a cascading effect through the system. Effects such as such as Hidden Failures (HF) in relays and operational errors can worsen system conditions and amplify the effects of a single failure [48]. Table 2.2 summarizes major blackouts in the past two decades.

Table 2.2: Summary of major blackouts in the past two decades.

| Year | Location        | Duration (hours) | Affected (millions) | Major Causes                                  |
|------|-----------------|------------------|---------------------|-----------------------------------------------|
| 2003 | USA/Canada      | 48               | 50                  | Critical software bug, protection malfunction |
| 2003 | Sweden/Denmark  | 6                | 4                   | Major faults, line overloads                  |
| 2003 | Italy           | 12               | 60                  | Frequency and voltage instability             |
| 2006 | Europe          | 3                | 15                  | N-1 violation, lack of coordination           |
| 2009 | Brazil-Paraguay | 7                | 60                  | Extreme weather                               |
| 2012 | India           | 15               | 620                 | Overloading, protection malfunction           |
| 2015 | Ukraine         | 6                | 0.26                | Cyber attack                                  |
| 2015 | Turkey          | 8                | 70                  | System failures, lack of coordination         |
| 2016 | Australia       | 6.1              | 1.7                 | Extreme weather                               |
| 2017 | USA             | 11               | 21                  | Weather and protection issues                 |
| 2019 | UK              | 2                | 1                   | Lightning and major fault                     |
| 2019 | Indonesia       | 9                | 21                  | Power plant disruptions                       |
| 2021 | Pakistan        | 9                | 200                 | Electrical fault                              |
| 2021 | USA             | 6                | 4                   | Winter storm                                  |
| 2022 | Bangladesh      | 10               | 140                 | Transmission line trip                        |

### 2.3 Connection Between Cascading Failures and Cyber Security

Large disturbances in power system operations can be followed by a series of events. If these events are not managed or controlled, they can lead to cascading failures and even a blackout. For a given power system with *n* components and *k* successive failures, the

number of successive failure of components is given by  $n^k$  combinations [6]. Thus, it is infeasible to check every combination. Nevertheless, cascading failure induced blackouts share some recurrent characteristics, such as: 1) Extreme weather and natural disasters [49], 2) Hidden Failures [39], [40], 3) System-level failures, and 4) Human errors. The focus of this work is limited to points 2 and 3, and how they may be triggered by cyber attacks. In a cascading failure sequence, power system dynamics plays a crucial role [50], [51]. A major disturbance or critical event in the power grid can cause a mismatch between power generation and demand, leading to the insecure operation of the system. Consequently, generators and transmission lines can get overloaded, causing the system frequency and voltages to drop. To keep the frequency and voltage within permissible limits, load shedding is often undertaken. However, if the curtailed load is not sufficient or if the action is delayed, additional transmission lines and generators may trip, leading to a domino cascading effect.

A complete cascading failure however, can take anywhere between minutes to hours, comprising of two distinct phases, i.e., ‘slow’ and ‘fast’ [42], [52]. This can be visualised through Figure 5 that illustrates the two phases for the USACanada 2003 blackout. The maximum damage is caused in the ‘fast’ phase, resulting in a domino effect which involves rapid tripping and disconnection of components. This phase typically occurs at the end of a cascading sequence, with a point of no return. It involves highly non-linear and dynamic phenomena, such as: 1) transmission line overloading, 2) generator disconnections, 3) frequency variations, 4) voltage instabilities, and 5) loss of synchronism. All these physical phenomena play a major role in the propagation of cascading failures. Power system dynamics can also be significantly affected by ICT infrastructure. This includes substation automation and protection systems, generator controls, protective relays, etc. With the looming threat of cyber attacks on power systems, impact assessment of cyber attacks on power system dynamics is a crucial topic. Hence, a detailed analysis of the key dynamic factors and phenomena influencing cascading failures is provided in the subsequent sub-section. This connection is also visualized in Figure 2.2.

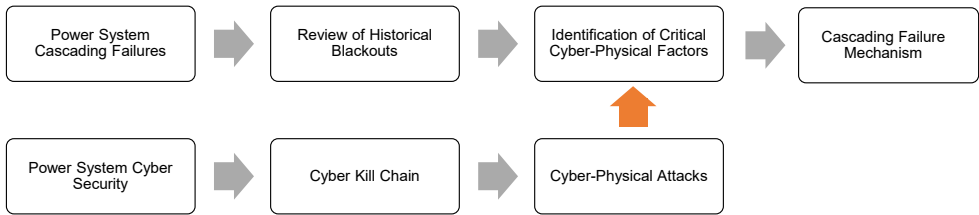


Figure 2.2: Connection between power system cascading failures and cyber security.

2.3.1 Cyber-Physical Factors

Loss of Transmission Lines

In almost all major blackouts, loss of transmission lines has played a major role [50], [55]. The main IEs before the cascade include excessive or unplanned power transfers, extreme

weather conditions, contact with vegetation, etc. There are various critical factors within this category that have contributed to real-world cascading failures, as follows:

- (i) **Zone 3 distance protection operation:** a crucial factor that has been repeatedly observed in many severe cascading outages is the erroneous operation of transmission line zone 3 distance protection. Under heavy loading, coupled with relatively low system voltage, a distance relay may confuse the overloading situation for an uncleared zone 3 fault as the impedance enters the third zone of protection. Such a phenomenon has been reported in the literature [49] and witnessed in real-world cascading failures and blackouts such as USA-Canada 2003 and Turkey 2015. Such a critical factor can be influenced by cyber attacks that spoof measurements of communication assisted protection schemes [22]. By altering the voltage and/or current measurements sensed by relays, it may be possible to maliciously trip them. Additionally, in the event of switching attacks and loss of multiple lines, this factor can be indirectly activated.
- (ii) **Line overloading:** when transmission lines are overloaded beyond their nominal limits, due to increased  $I^2R$  losses, they start to sag and dissipate massive heat. This involves both thermal and electrical phenomena. If left unchecked beyond a certain time duration, they are automatically tripped by overload protection. In the worst case, overhead lines can sag, come in contact with vegetation, and trip due to flashovers. Therefore, line overloading can set off a cascading chain; other parallel lines in the system may get overloaded as well and trip, thereby severely compromising system integrity. It is noted that overhead line overloading is a ‘slow’ phenomenon, in comparison to other dynamic parameters and categories discussed subsequently. Line sags and flashovers can take anywhere from between minutes to hours. Interestingly, the cascading failures propagate non-locally, i.e., the initiating event could be a significant distance away from subsequent line trips [28]. This loss of lines not only disconnects equipment but also leads to system parameters such as voltage and frequency going out of their limits.

By gaining access to the substation controls and opening multiple circuit breakers at once, lines can be put of service, as seen during the Ukraine 2015 attack. Consequently, parallel lines will be overloaded. If the original lines are not put back into service in a timely manner, the overloaded parallel lines can also trip, initiating a domino effect and possibly a voltage collapse. This can have a particularly devastating effect on the entire power system, as observed in both Italy and USA-Canada in 2003 [45].

### Voltage Stability

Maintaining the system voltage at nominal values is crucial to ensure secure system operation. The fundamental reason for voltage instability is the inability to satisfy reactive power demands. Consequently, reactive power losses can increase, leading to voltage sags. During a cascading failure process, due to sudden and rapid tripping of elements, bus voltages can change drastically, causing severe voltage instabilities. Also, changes in active or reactive power outputs of generators can cause power swings and reactive power issues, respectively. Therefore, either primary or backup protection relays can trip, setting off a

voltage collapse. This typically activates Under- Voltage Load Shedding (UVLS) or protection schemes that disconnect elements due to extremely low voltage levels. In the absence of sufficient voltage levels, the entire power system collapses, resulting in a blackout. The critical factors affecting voltage stability during a cascading failure are as follows:

- (i) **Reactive power compensation:** the crux of voltage instability is improper reactive power compensation. Devices for reactive power support such as Static VAR Compensators (SVCs) and Static Compensators (STATCOMs) can be targeted by Man-in-the-Middle (MITM) or data modification attacks to alter reactive power injections [33, 35]. In the worst case, this can induce severe voltage instabilities and lead to a voltage collapse.
- (ii) **Voltage regulation:** mechanisms to regulate voltage such as tap changers can also be compromised to impact voltage stability. In future power systems, the increased presence of Distributed Energy Resources (DERs) also provides an additional attack surface. These DERs are expected to be networked to the grid edge, via IoT that are also vulnerable. For example, [50] discusses the exploitation of vulnerabilities in photovoltaic inverters to cause abnormal voltages, and associated remedial measures to avoid this situation.
- (iii) **Generator excitation:** for any grid-tied synchronous generator, voltage/VAr control is provided by the Automatic Voltage Regulator (AVR) by varying field excitation current. Therefore, generators can be under or over excited, depending on voltage support requirements [51]. In the event of over or under excitation, the AVRs of generators can trip for safety reasons. This can potentially instigate voltage stability issues in the case of other contingencies. Such an advanced cyber attack scenario, targeting generator AVRs is discussed in [52].

### Transient Stability

The most impactful event in a cascading failure is the disconnection of generator units and loss of synchronism. Without sufficient power production, the power grid can destabilize rapidly. The major factors contributing to transient instabilities in cascading failures are the following:

- (i) **Fault-clearing times:** the primary requirement for transient stability is the satisfaction of the equal-area criterion, i.e., the kinetic energy absorbed by the generator rotor during acceleration or fault conditions must equal the kinetic energy dissipated during deceleration, post-fault. Hence, it is crucial that faults must be cleared as quickly as possible to prevent loss of synchronism. Therefore, a cyber attack that manipulates protection schemes and their associated communications to cause increased fault clearing times can lead to loss of synchronism. This may be possible through Denial-of-Service (DOS) attacks which delay the communication of critical control commands, as discussed in [15, 53].
- (ii) **Loss of generation:** in cascading failure events, angular instabilities may arise due to sudden large component disconnections or system changes, resulting in rotor angle instabilities. The sudden loss of a large generator or line switching can induce transient instabilities. As discussed in [21, 54], targeting the breaker controls of a

generator and rapidly switching them out of phase can result in transient instabilities. Consequently, the generator can lose synchronism and get disconnected or even damaged.

- (iii) **Generator controls:** crucial aspect to ensure transient stability is the terminal voltage of generators, controlled by the AVR through field excitation. Hence, a cyber attack altering the field excitation parameters can affect transient stability of the system. This is especially true in the case of coordinated attack, leading to loss of multiple components. Typically, generators are equipped with several interface protection relays, and schemes to safeguard them in the event of major fault conditions. However, during a cascading failure process, the very same protection relays, while ensuring the safety of the generator can compromise the rest of the system. This directly worsens the cascading process in the rest of the system.

Switching attacks on generators are extensively discussed in [55]. This research shows how cyber attacks can disconnect generators and initiate cascading failures. Furthermore, [21] demonstrates the physical implications of such cyber attacks on the machine and power system. Hence, a cyber attack seeking to compromise transient instability can rapidly connect and disconnect the generator's main circuit breaker. Such an advanced attack can destabilise the entire power system in a matter of a few seconds. This can result in a loss of synchronism in the remaining parts of the system. Subsequently, other generator units may be tripped, resulting in a large-scale blackout, possibly requiring significant amounts of restorative efforts.

### Frequency Stability

The root cause of frequency instability is a mismatch between supply and demand. This can manifest in multiple ways, as follows:

- (i) **Islanding:** cascading failures involve transmission line overloading and tripping of connected generators. This may result in islanding, i.e., creation of areas with a large mismatch between power supply and demand. As a result, the frequency within the islanded systems can differ vastly. This can also occur due to sudden large load disconnections. Depending on the inertia of the synchronous generators within the system, such a mismatch can activate Rate of Change of Frequency (ROCOF) protection to protect the generator units. With the influx of more renewable power generation, system inertias are expected to reduce further. Therefore, ROCOF protection is a critical parameter with regard to frequency stability and cascading failure analysis. A resonance cyber attack targeting ROCOF and load frequency control of generators is discussed in [56]. In this type of attack, the adversary modifies the input signals to generator controllers based on a resonance source, e.g., ROCOF. This results in a negative feedback on load frequency control, such that the targeted generator loses stability. Furthermore, the authors conclude that the maliciously modified inputs still lie within the normal operating range, thereby making the attack highly stealthy.
- (ii) **Supply-demand mismatch:** to cause a mismatch between supply and demand, multiple cyber attack strategies are possible. Some sophisticated cyber attacks to induce such mismatches are discussed in the literature. In [57], the authors explain

how botnets may be used to rapidly increase power demand before frequency control mechanisms can react. Using a hypothetical example of continental Europe, they show how this can lead to loss of load and generation. Likewise, [58] presents a cyber attack scenario to artificially manipulate power demand through a spoofed market price signal. The net result in both cases is that of sudden frequency variations, prompting remedial actions such as load shedding.

- (iii) **Load shedding:** to prevent scenarios such as islanding, corrective actions such as Under Frequency Load Shedding (UFLS) techniques are undertaken, leading to a loss of load, thereby creating a power imbalance. Such techniques must be fast enough to restrict the frequency drop, otherwise, the system can further destabilise. Sustained under frequency or over frequency conditions can cause generators to automatically trip. Therefore, a DOS cyber attack which causes a delay in communication of load shedding commands can have an adverse effect on frequency stability, as discussed in [59].

It is to be pointed out that all of the aforementioned and discussed categories and factors are not mutually exclusive, but intertwined. For example, transient and voltage instabilities are strongly linked and usually occur together [51]. Likewise, frequency instability and transient instability also influence each other. It is worth mentioning that cyber attacks exploiting even one of the critical categories may induce cascading failures due to the strong interplay between all the phenomena. Extending this line of thought, a coordinated cyber attack can therefore accelerate the cascading failure mechanism. A recent study has confirmed this acceleration mechanism being observed in major historical cascading outages [13]. As a result, in the event of a coordinated cyber attack, the power grid may reach a point of no return sooner, triggering a massive collapse. A brief summary of cyber attacks from the literature targeting critical factors is presented in Table 2.3.

Table 2.3: Summary of cyber attacks targeting critical factors.

| Categories                 | Factors                       | Cyber Attacks |     |        |           |          |          |
|----------------------------|-------------------------------|---------------|-----|--------|-----------|----------|----------|
|                            |                               | MITM          | DOS | Replay | Switching | Spoofing | Economic |
| Loss of transmission lines | Zone 3 distance protection    |               | ✓   |        | ✓         | ✓        |          |
|                            | Line overloading              | ✓             |     |        | ✓         | ✓        | ✓        |
|                            | Protection malfunction        | ✓             |     | ✓      |           | ✓        |          |
| Voltage instability        | Reactive power compensation   | ✓             |     | ✓      |           | ✓        |          |
|                            | Voltage regulation            | ✓             |     | ✓      |           | ✓        |          |
|                            | Line overloading              | ✓             |     |        | ✓         | ✓        | ✓        |
|                            | Generator excitation controls |               |     | ✓      |           | ✓        |          |
| Transient instability      | Fault clearing times          | ✓             | ✓   |        |           | ✓        |          |
| (Loss of synchronism)      | Loss of generation            | ✓             |     |        | ✓         |          |          |
|                            | Generator excitation controls |               |     | ✓      |           | ✓        |          |
| Frequency instability      | Islanding                     | ✓             |     |        | ✓         | ✓        |          |
|                            | Power mismatch                | ✓             |     |        |           |          | ✓        |
|                            | Load shedding                 |               | ✓   | ✓      |           |          | ✓        |

## 2.4 Cyber Attacks Enabling Cyber-Physical Factors

Cyber attacks on power grids have emerged as a sophisticated modern-day threat with wide-ranging ramifications. They are High-Impact Low-Frequency (HILF) events that can severely impact power system operation and stability. Table 4 lists some well-reported cyber attack exploits from literature, specifically targeting power systems. Such attack vectors are mainly inspired by the real-world cyber attacks in Ukraine in 2015 and 2016. Figure 6 depicts a brief timeline of major cyber attacks on industrial control systems.

### 2.4.1 Cyber Kill Chain

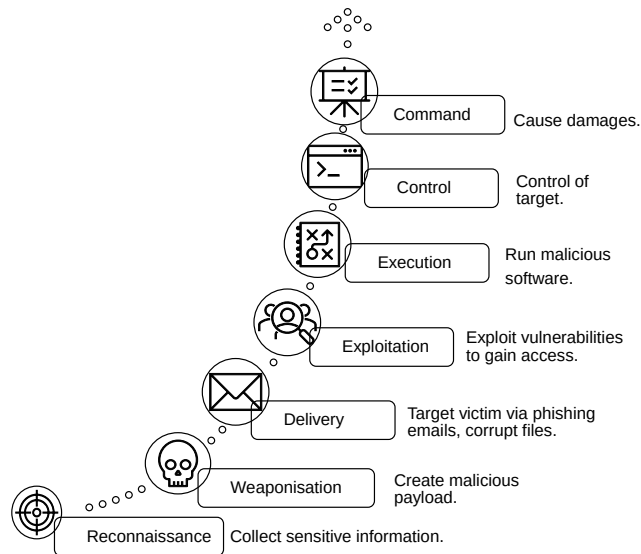


Figure 2.3: Cyber attack kill chain on critical infrastructures.

In this chapter, we focus our discussions on cyber attacks aimed at causing large-scale cascading failures and blackouts. Such cyber attacks can broadly be categorised into four categories:

1. Attacks affecting physical equipment.
2. Attacks targeting communication networks.
3. Application-centric attacks.
4. Data-centric attacks.

All the subsequently discussed cyber attacks fall into one of the four categories. As previously discussed, most cascading failure induced blackouts consist of a multitude of factors. However, the critical factors that influence system dynamics and lead to the domino effect are limited. Therefore, in subsequent subsections we discuss how said factors can be exploited through different hypothetical 'nightmare' cyber attack scenarios. These scenarios are aimed at initiating or accelerating cascading failures, by influencing system

conditions. The type and nature of the exploits are based on cyber attacks on power grids, already reported in the literature. The goal of this discussion is to highlight how such attacks can lead to cascading failures and a blackout. Hence, most advanced cyber attacks on ICS follow a similar chain of events, with the following steps:

1. **Reconnaissance.** This is the first stage in the cyber attack kill chain and involves conducting investigations of the target. Through this step, the adversary collects sensitive/critical information that can be used to jeopardize the target. An example for such information could be network data, critical equipment locations, etc.
2. **Weaponization.** The information collected from the first stage is then used to develop an appropriate attack vector or payload. This is referred to as the weaponization stage. An example of such a payload could be a malware or a bot.
3. **Delivery.** The third stage in the kill chain is the delivery stage. Once the payload is ready, the victim is targeted through suitable means. This may include mechanisms such as phishing emails, corrupted file attachments, malicious hyperlinks, etc. The goal of this stage is to successfully infect one or more machines of the target with the malicious payload.
4. **Exploitation.** The fourth stage entails exploitation of system resources through the delivered payload. An attacker can exploit known vulnerabilities in the target environment through the payload, to gain backdoor access to entire critical infrastructures.
5. **Execution.** This is the actual attack phase of the kill chain. Having gained unauthorised access, an adversary can then run their malicious code, remotely, to wreak havoc on the target.
6. **Command and Control.** These stages involve the adversary taking over controls of critical infrastructures and manipulating them to cause serious damages. Such actions could include changing operating set points, shutting down entire components or systems, thereby leading to catastrophic damages. Examples of such unauthorised actions with respect to power grid operations can include malicious opening of circuit breakers and manipulation or spoofing of controller set points of generator AVR and governors. The cyber attack kill chain and associated stages are illustrated through Figure 2.3.

### 2.4.2 Malware Attack

There are well known examples of malware targeting and compromising functioning of ICS. This includes the Stuxnet virus [60], Blackenergy 3 [1], and 'Crashoverride/Industroyer' [2]. The last two were responsible for the cyber attacks, specifically targeting the power grid in Ukraine in 2015 and 2016, respectively. In April 2022, cyber attacks caused a malfunction in the communication systems used for monitoring and control of nearly 2000 wind turbines in Germany. Around the same time, the Ukrainian computer emergency response team confirmed that high-voltage electrical substations in Ukraine were targeted by Industroyer2 malware. These incidents highlight the evolving cyber threat landscape. Malware attacks on physical equipment can affect the availability and integrity of signals, thereby compromising the system integrity. For example, a compromised critical device

may continue to operate slowly than what is required by the corresponding application, even though the signals produced are reflective of the actual system, which triggers usability concerns. Hence, an advanced malware attack can wreak havoc on power system operations.

In this attack scenario, it is assumed that the adversary has gained access to the IT/OT infrastructure of the target power grid operator through malicious hacking activities, similar to the Ukraine 2015 attack [1]. The adversary then stays within the system, monitoring and recording system operations to pick an appropriate attack target and timing. This corresponds to stages 1, 2, and 3 in the cyber kill chain. In the summer, the power system is operating close to its limits due to a high demand. This prompts the attackers to launch their attack. The attackers having conducted reconnaissance are familiar with the grid topology and operational conditions. They execute the first stage of the attack by planting a sophisticated malware, similar to Industroyer that initiates a race condition, given their access to the IT/OT infrastructure. This results in a critical software bug that goes unnoticed. It is assumed that the first stage is carried out well in advance. Hence, most, if not all regional control centres are infected by the malware. The goal of this stage is to blindside the system operator and cause lack of situational awareness. The malware prevents timely remedial actions in case of major faults or disturbances. Consequently, even a single IE can become a critical event, setting off a catastrophic cascading effect.

In the second stage of the attack, at a major transmission substation, where some lines are out of service for maintenance, the attackers take over the substation controls. They initiate automatic opening of all circuit breakers, even going to the extent of blocking all manual overrides. This corresponds to the execution and control stages of the cyber kill chain. Due to the malware, the system operator is fed misinformation that the system is in a healthy state. By opening all breakers in this substation, the already stressed system is pushed close its limits. Parallel lines in neighbouring substations are soon overloaded, causing line sags and eventual flashovers. A critical transmission line interconnecting the northern and southern regions is put out of service due to the cyber attack.

This forms the critical event and sets off a domino effect. Due to the sudden power imbalance and frequency instability, islands are formed. Consequently, under frequency relays of generators start to trip. This worsens system conditions and causes huge load disconnections. Subsequently, the lack of generation and extremely poor voltage levels leads to a blackout. The entire sequence of events is summarised in Table 5. The blackout from the initial event takes 1 hour. The critical cascading events happen in a matter of a few minutes. A similar sequence of events is what transpired during the USA- Canada blackout of 2003 [45].

### 2.4.3 Operational Technology Hijacking

As shown by the cyber attack in Ukraine, 2015, malicious takeover of substations and SCADA system can lead to catastrophic consequences [19, 61]. Through lateral movement from IT to the OT system, attackers hijacked the substation OTs and maliciously disconnected multiple circuit breakers from the control centre. Such an attack vector is possible due to the use of legacy power system communication protocols with limited or no cyber security implementations. These communication protocols used by utilities, such as Distributed Network Protocol 3 (DNP3) and IEC 104 are vulnerable [19, 62, 63]. Particularly,

Table 2.4: Sequence of events due to malware attack.

| Time (hrs.) | Event                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22:10:05    | Cyber attack at a transmission substation. Five circuit breakers are disconnected and manual override is disabled. This forms an N-k contingency. The system is highly stressed. |
| 22:10:05    | Critical transmission line is put out of service due to the cyber attack. Power flows are rerouted through other parallel lines.                                                 |
| 22:50:07    | Automatic Under frequency Load Shedding (UFLS) initiated. System operator finally realises situation due to load disconnections and emergency calls.                             |
| 22:55:10    | Cascading failures propagate and affect generating units. Under frequency protection automatically disconnects multiple generators due to sustained low frequency conditions.    |
| 23:00:00    | Extremely poor voltage profile leads to voltage collapse and blackout.                                                                                                           |

through eavesdropping and active reconnaissance, attackers can jump from the substation to the control centre. In a critical ICS infrastructure, such attacks can have serious consequences, as timely operation is strictly necessary. This is shown Figure 8, wherein, critical messages/commands between control centre and substations can be sniffed or hijacked to gain unauthorised access. In the worst-case, such attacks can maliciously disconnect lines and equipment in the power grid. This can set off a chain of contingencies that may lead to cascading failures and even a blackout.

In the imagined attack scenario, it is assumed that the cyber attackers have gained backdoor access to the gateway server in multiple substations through spear phishing or malware attack [62]. This server acts as the medium of communication between the control centre and substation. Thereby, by gaining access to the server, the communication channel is compromised, allowing the adversaries to monitor and inspect all traffic. This corresponds to steps 1 and 2 in the cyber kill chain. The attackers inspect the type and content of all packets exchanged between the control centre and compromised substations, over an extended period of 3-4 months.

In stage two, with this knowledge, the attackers launch their cyber attack. The particular target utility uses IEC 104 for their SCADA communications. The attackers jump from the substation to the control centre by exploiting known IEC 104 vulnerabilities. From the control centre, the attackers disable manual overrides, launch spoofed packets that tamper with the tap positions of the transformers within the substations. This has a severe effect on the voltage stability of the entire system as voltage levels are severely affected. A sustained low-voltage condition results in undervoltage load shedding schemes being activated. Additionally, the attackers also maliciously open multiple circuit breakers, thereby disconnecting several transmission lines and loads. Such a coordinated attack has an acute effect on voltage and frequency stability, initiating a voltage collapse. Generators are tripped by their over exciters due to high reactive power outputs. The cascading event propagates rapidly, causing successive line overloads and trips, resulting in a blackout.

2.4.4 False Data Injection

The most commonly reported type of cyber attack on power systems in literature is the False Data Injection (FDI) attack. An FDI attack operates under the assumption that an

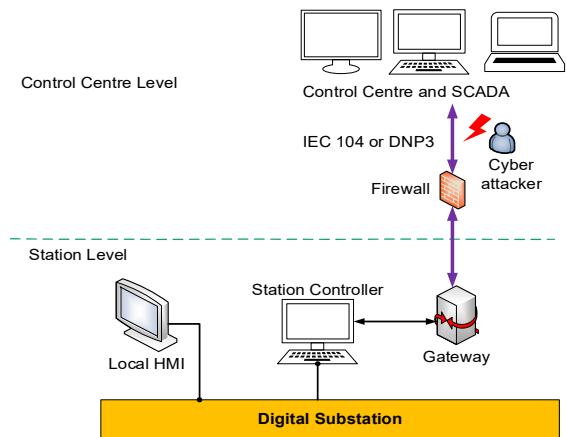


Figure 2.4: OT hijacking attack.

Table 2.5: Sequence of events due to OT hijacking cyber attack.

| No. | Event                                                                                                                                                             |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Cyber attack at three substations. Transformer tap positions are tampered causing changes to voltages.                                                            |
| 2.  | Generators automatically increase VAr outputs. System operator is sent spoofed packets from compromised substations.                                              |
| 3.  | Automatic UVLS is activated to alleviate low voltages.                                                                                                            |
| 4.  | Attackers open multiple feeder circuit breakers at once, disconnecting numerous lines and loads.                                                                  |
| 5.  | Sudden disconnections cause power swings and frequency instabilities. Generators are tripped by automatic overexcitation protection due to voltage instabilities. |
| 6.  | UFLS is activated to arrest frequency drop due to loss of generation.                                                                                             |
| 7.  | Three parallel overhead lines are overloaded beyond thermal limits and trip.                                                                                      |
| 8.  | Severe frequency and voltage instabilities cause cascading failures and blackout.                                                                                 |

attacker can access current power system configuration information and manipulate the measurements of meters at physically protected locations such as substations. Thereby, they may introduce arbitrary errors into certain state variables without being detected. Most FDI attacks reported in literature are aimed at targeting state estimation algorithms and measurements [64, 65]. Related work also discusses data-driven attacks that target power flow measurements [66]. Such attacks however, are limited or restricted to boundaries of one substation. Hence, we focus our attention on data integrity attacks that target specific components of power systems to cause widespread damages.

Data integrity attacks targeting power system protection, i.e., relays and communication are of serious concern. It is critical to ensure security of supply and maintain power system health. With rapid developments in ICT and digital technologies, conventional pro-

tection systems are being upgraded into communication-assisted protection schemes [67]. Such communication-assisted protection schemes provide high-speed tripping at either ends of a protected line. Traditional multi-zone distance protection lacks such capabilities. Furthermore, reduced fault clearing times can minimise power system instability conditions and improve system reliability. Such high-speed fault clearing is achieved through dedicated communication between line terminals. Each line terminal communicates its status as a data bit to the remote end(s), over a dedicated communication channel. The data bit can represent either a trip or block command, depending on the protection scheme being employed. The most commonly used schemes are Permissive Overreaching Transfer Trip (POTT) and Permissive Under-reaching Transfer Trip (PUTT) [68]. While offering aforementioned advantages, this digitalization of protection raises cyber security concerns [69].

Cyber attacks considering the role of protection systems are extensively discussed in [67]. Typically, the most commonly used protection schemes are distance and differential protection for protection of transmission lines and transformers, respectively. Cyber attack vectors targeting these schemes are reported in [68, 69]. Such sophisticated cyber attacks manipulate the parameters sensed by protection relays to calculate trip conditions. Thus, a successful cyber attack can lead to malicious tripping of relays, while remaining undetected. Such attacks can have crippling consequences on power system operations. They can directly result in unwanted opening of circuit breakers, leading to transient instabilities. Another possibility is a ‘sleeper cell’ attack. In this scenario, the protection equipment is inhibited or blocked from normal functioning. Hence, during a fault condition, the relay may not operate, causing other zones of protection to be activated. This can subsequently cause other unwanted relay trips, triggering a cascading effect. While sounding far-fetched, such cyber attack scenarios are worrisome, since protection issues and malfunctions are directly/indirectly involved in about 70% of cascading failure incidents [50].

In the attack scenario, we consider two types of attack manipulations. The first one is focused on directly modifying the relay parameters used to issue tripping commands. The second is inhibition of protection functionality. The latter can be achieved by carrying out DoS attacks on the communication channel used by communication-assisted protection. In the considered cyber attack scenario, attackers have gained access to the communication channel used by the communication-assisted protection system at three substations. This corresponds to steps 1-3 in the cyber kill chain. Execution of a DoS or FDI attack requires a malicious device with access to communication channels used by the relay. By remotely introducing such a device into the network, attackers can access the communication channel which enables fast breaker actions during faults. By launching a cyber attack when timely breaker action is necessary, however, they cause substantial disturbances to the power grid. This forms the crux of the discussed cyber attack scenario.

The attackers launch a DoS attack by flooding the communication channel with packets through their own malicious device. This results in blocking of permissive trip communications, i.e., prolonged fault clearing times. Subsequently, transient instabilities may arise in case of major faults. As the second stage of the attack, the cyber attackers execute an FDI attack to modify the trip signals. The attackers issue spoofed permissive trip signals that cause malicious tripping of relays. Now, when a fault occurs in the associ-

ated transmission line, due to the DoS attack, it is not cleared on time. Simultaneously, through the FDI attack, multiple relays are maliciously tripped, causing sudden opening of circuit breakers. Both these conditions put together induce massive system instabilities, initiating a domino effect, i.e., cascading failures and a blackout. The sequence of events is summarised in Table 7.

Table 2.6: Sequence of events due to DoS and FDI attacks.

| No. | Event                                                                                                                                                                                        |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | DoS attack on communication-assisted protection of a critical transmission line. Timely protection functionality is jeopardised.                                                             |
| 2.  | During short circuit, due to the DoS attack, zone 1 tripping is blocked. Zone 2 and 3 protection activated. Results in transient instabilities.                                              |
| 3.  | FDI attack is executed, and multiple relays issue malicious permissive trip signals. Multiple transmission lines suddenly disconnected, resulting in an N-k contingency.                     |
| 4.  | Two or more regions are islanded by ROCOF protection as a consequence of the cyber attack.                                                                                                   |
| 5.  | Mismatch between generation and demand in the regions causes frequency drops. Automatic UFLS is activated in steps. System is split into two asynchronous regions and partially blacked out. |

### 2.4.5 Advanced Persistent Threats

Advanced Persistent Threats (APTs) represent a significant cyber security challenge for critical infrastructures, such as power systems. APTs are highly sophisticated and stealthy forms of cyber attacks conducted by well-funded and persistent threat actors. In the context of power systems, APTs pose a grave risk due to their potential to disrupt essential services, compromise data integrity, and even inflict physical damages. TABLE 7. Sequence of events due to DoS and FDI attacks. They are characterised by three main aspects:

1. **Persistence:** APTs are carried out over a long-term, with stealthy presence in a targeted OT network or system. Threat actors maintain access and continue their reconnaissance over an extended period, often remaining undetected.
2. **Sophistication:** APTs employ advanced techniques, including zero-day exploits, custom malware, and social engineering tactics. They adapt to network defences and conditions, making them difficult to detect and mitigate.
3. **Targeted:** APTs are not opportunistic attacks but rather meticulously planned and specifically aimed at high-value targets and critical infrastructures, such as power grids.

APTs pose a grave threat to the power system operation, as shown in the Ukraine 2015 and 2016 cyber attacks. Unlike cyber attacks on IT systems, attacks on cyber-physical power systems can lead to operational disruptions, with physical impact such as cascading failures and power outages [70]. In conclusion, APTs on power systems represent a serious and evolving threat that necessitate proactive cyber security measures. By understanding their characteristics, motivations, and potential impacts, utilities can better prepare and defend against these sophisticated cyber threats.

## 2.5 Conclusions

The key outcomes of this chapter can be summarized as follows. Furthermore, based on this study, the following chapter presents in-depth, cyber security of digital substations and its impact on power system dynamics.

### RQ1.1 How to show qualitatively that cyber attacks can cause cascading failures?

This chapter presented a fundamental analysis of the link between the power system cascading failure mechanism and cyber security. This was achieved through a comprehensive state-of-the-art review of major historic power system blackouts caused by physical disturbances. Based on this, critical cyber-physical factors that enable and influence the cascading failure mechanism were identified. Furthermore, hypothetical cyber-physical attack scenarios were developed to analyze the effects of the critical factors through different cyber attack vectors. A systemic evaluation of the scenarios revealed how cyber attacks can initiate cascading failures, leading to a blackout. Findings of this chapter highlight the direct link between cyber attacks and their influence on critical factors in the cascading failure mechanism.



## 3

## 3

## Cyber Security of Digital Substations: Impact Analysis and Mitigation

*IEC 61850 is a power system automation and communication standard that forms the basis for digital substations. It enables real-time communication and data exchange between critical substation automation and protection devices within digital substations. However, IEC 61850 is not cyber secure. In this chapter, we discuss the cyber security of digital substations and related implications on the operation of the grid. Cyber attacks may exploit the vulnerabilities of the Sampled Values (SV) and GOOSE protocols of IEC 61850. The cyber attacks may be realized by injecting spoofed SV and GOOSE data frames into the substation communication network at the bay level. We demonstrate that such cyber attacks may lead to obstruction or tripping of multiple protective relays. Coordinated cyber attacks against the protection system in digital substations may cause generation and line disconnections, triggering cascading failures in the power grid. This may eventually result in a partial or complete blackout. The cyber attack model, impact on power system dynamics and cascading failures are verified experimentally through a proposed cyber-physical experimental framework that closely resembles real-world conditions within a digital substation, including IEDs and protection schemes. Lastly, mitigation measures to prevent these types of attacks using hash-based message authentication codes as specified by the IEC 62351-6 standard are implemented and discussed.*

---

This chapter is partly based on the following publications:

▣ V. Rajkumar *et al* "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in *Proc. 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020, pp. 247-254.

▣ V. Rajkumar *et al* "Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis," in *Proc. 2020 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Sydney, NSW, Australia, 2020, pp. 1-6.

### 3.1 Introduction

Power system automation and communication standards are spearheading the power system transition towards a smart grid. However, this increased power grid digitalization raises questions, especially with regard to, vulnerabilities and cyber secure operation of the smart grid [3, 14]. IEC 61850 is a power system communication standard used for substation automation and protection in digital substations. It enables information exchange through different communication protocols, two of which are covered in this chapter. The GOOSE and SV protocols are used to communicate substation events and measurements within a substation, respectively. Although it provides increased benefits, IEC 61850 is not cyber secure. The standard does not implement any encryption due to strict real-time requirements of protection signals, typically in the range of 3-4 ms. This makes it highly susceptible to cyber attacks. The exploit of GOOSE protocol vulnerabilities within IEC 61850 is demonstrated in [71, 72]. It is a cause for serious concern that such cyber security vulnerabilities maybe exploited by potential attackers. Cyber attacks on power grids are a real modern-day threat. On December 23, 2015, cyber attacks were carried out on the power grid in Ukraine. Seven 110 kV and twenty-three 35 kV power substations were disconnected from the grid for hours. These attacks were the first publicly acknowledged cyber incidents to result in power outages that affected about 225,000 customers [1]. Thus, cyber security of power systems has become an important area of research [17].

### 3.2 Power System Protection and Automation

The main objective of power system protection and automation is to ensure system stability and security. Power system protection schemes are based on multi-purpose digital relays. In addition to protection functions, the digital relays can communicate with control centres, perform control actions, and log data from system events. Within the scope of this chapter, the following protection schemes are covered.

#### 3.2.1 Distance Protection

The most widely used protection scheme for transmission systems is distance protection. The distance relay operates on the principle of comparing the line voltage and current to obtain their ratio. Typically, for transmission line protection, a relay's instantaneous tripping zone, i.e., zone 1, is set with a reach of 80-90% of the line impedance. This corresponds to 80-90% of the physical line length. Faults beyond that point on the line, i.e., at the far end, are tripped by the next protection zone, i.e., zone 2. The second zone also includes a time delay, usually set between 150 to 400 ms. This setting is recommended to be above 120% of the line impedance, in order to provide enough safety margin for faults at the extreme ends of a transmission line.

#### 3.2.2 Out of Step Protection

Out of step protection is implemented at the interface of synchronous generators with the power grid, to avoid prolonged asynchronous operation. It uses the rate of change of impedance to determine a power swing condition and the resulting out of step operation. Due to large variations in voltages and currents during an asynchronous condition, other protection functions, such as distance protection, are blocked if a power swing is detected.

This is done in order to avoid improper operation of the relays. In predetermined parts of the system, out of step protection is usually set up to contain disturbances through controlled islanding of the power grid.

### 3.2.3 Frequency and Voltage Protection

If the power system is heavily loaded, then an unwanted or unforeseen trip can lead to substation voltages going out of limits for nominal system operation. In order to restore the system voltages to nominal conditions, Under Voltage Load Shedding (UVLS) schemes are employed. Once the voltage drops below what is an acceptable threshold, e.g., 0.90 p.u., the protection function is activated and results in load disconnections from the grid. Typically, the load sheds occur in percentage increments of total load demand with certain time delays, usually in the range of a few seconds. Therefore, in theory, cyber attacks on IEDs serving as protection devices within substations can result in disconnection of generators or lines. This sudden disconnection of lines or generators from the system can lead to a deficiency in generation or load, causing fluctuations in the system frequency. Subsequently, this can result in load shedding. In most power systems, an Under Frequency Load Sheddings (UFLSs) system is in place. Load is usually shed in multiple increments with predetermined time delays. Conversely, with large load disconnections, the governors of the generators may not be fast enough to react. For this case an over frequency protection is implemented. This protection is based on a frequency-time curve depending on the type of generation units. For most types of power- plants, the immediate disconnection of the plant happens at 10% higher than nominal frequency. Since cyber attacks aim at opening circuit breakers unexpectedly, they can result in unwanted load shedding and generation disconnection.

## 3.3 IEC 61850 Standard

IEC 61850 is a modern power system communications standard that serves as the foundation for an open communication and data-exchange within digital substations. These substations are an integral part of the smart grid paradigm. A digital substation replaces analogue copper wiring with digital Ethernet that offers a plethora of benefits, not limited to improved measuring accuracy, ease of device configuration, and real-time performance. This is achieved through the IEC 61850 standard which defines a vendor agnostic data exchange architecture applied to substation automation and protection systems. This allows for the interoperability of devices from different vendors. The following sections provide a summary of the standard, two of the studied protocols within this thesis, cyber security vulnerabilities affecting them, and mitigation measures to address them. The IEC 61850 standard defines a vendor agnostic data-exchange architecture applied to substation automation and protection systems. This allows for the interoperability of devices from different vendors. Further, it adopts existing standard communication protocol stacks and services. Over the years, IEC 61850 has grown out of substation boundaries to even cover substation-to-substation and substation-to-control centre applications. Furthermore, it enables information exchange through different communication protocols, two of which are covered extensively in this chapter. The GOOSE protocol is used for communicating critical events in real-time, e.g., tripping commands between two or more protective relays,

while measurements are communicated using the SV protocol [73], both using Ethernet multicast. The layout of a typical digital substation is illustrated in Figure 3.1. This comprises of station, bay, and process levels. A local area network enables the communication between engineering workstations, station control systems, and communication servers with control centres.

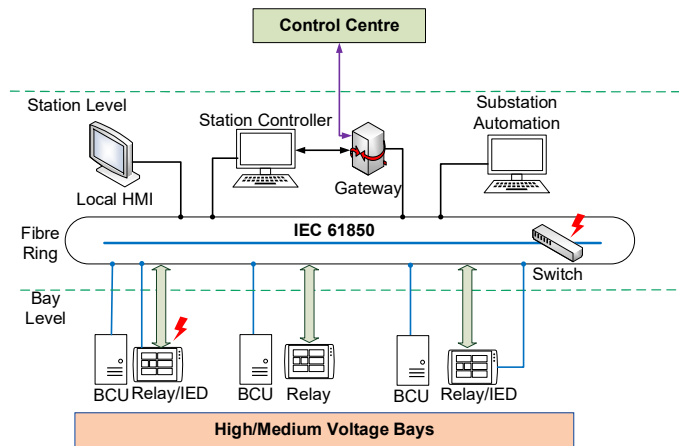


Figure 3.1: Digital substation architecture.

### 3.3.1 Generic Object Oriented Substation Event

IEC 61850 GOOSE is a communication protocol used in digital substations for real-time, high-priority messages. It is part of the IEC 61850 standard, developed to provide a comprehensive framework for substation automation and the interoperability of equipment from different manufacturers. GOOSE messages are used to transmit time-critical information, such as protection signals or equipment statuses, between IEDs within a substation. This allows for fast reaction to faults or other system events. Unlike traditional polling-based communication, GOOSE uses event-driven messaging, i.e., when a change in the status of a monitored component occurs (for e.g., circuit breaker open/close, fault detection), a GOOSE message is immediately sent to notify other devices. Additionally, GOOSE messages are sent over the network using Ethernet multicast, allowing multiple IED to receive the message simultaneously. This is crucial for ensuring fast communications between devices without having to establish one-to-one connections. As a result, GOOSE messages are designed for low latency (in the millisecond range), enabling them to trigger protective actions quickly, such as isolating faulty equipment. Consequently, GOOSE communication is unacknowledged, meaning there is no handshake or confirmation of receipt. This is a trade-off for speed, making it more suited for protection and control systems where fast responses are more important than confirmation successful message delivery [71, 74].

The structure of a typical GOOSE message/frame is shown in Figure 3.2. It includes the physical link destination and source addresses, i.e., Media Access Control (MAC) tag

of the Virtual Local Area Network (VLAN), type header, length of the frame, and data payload. Under the data payload, the status and sequence number fields, i.e., stNum and sqNum, in the GOOSE message are often considered as basic security mechanisms. In the processing algorithm for GOOSE, each time a GOOSE message is sent, the sequence number is incremented by 1, with a maximum value of  $2^{32}$  (an unsigned 32-bit integer) before it resets to 1. When an event occurs at a substation, such as a trip signal, the update frequency of GOOSE messages increases to ensure successful delivery. In this event mode, the transmission time falls between 0.5 and 5 milliseconds. Additionally, the status number is incremented by one, and the sequence number is reset to zero. Therefore, incoming GOOSE messages with a lower status number than the current one are not processed and the frame is discarded.

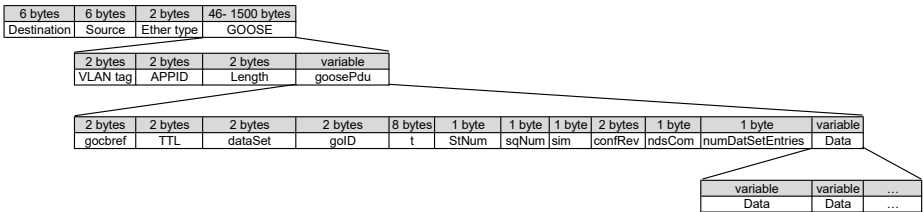


Figure 3.2: Structure of a GOOSE protocol message.

### 3.3.2 Sampled Values

IEC 61850 SV is a communication protocol that enables the communication of analog measurements in digital form within electrical substations. Sampled Values are typically used to transmit measurements like currents, voltages, and other power system parameters from primary equipment, for e.g., current transformers (CTs) or voltage transformers (VTs) to protection and control devices such as IEDs. Sampled Values are transmitted via multicast Ethernet frames, similar to GOOSE. This allows different IEDs, such as protective relays, control systems, or data recorders, to receive the same measurement data in real-time. Furthermore, sampled values have high sampling rates, for e.g., 80 samples per cycle for a 50/60 Hz power system, thereby providing detailed and accurate measurements necessary for protection and control systems. These high sampling rates help detect and respond to transients and faults within the power system. While the SV protocol is not as sensitive to latency as GOOSE, it transmits messages at a high data-rate of up to 4.8 kHz, equating to an interval of 0.2083 ms between each SV message. With an average SV message size of 120 bytes, this results in traffic throughput of  $\approx 0.576$  Mbps. The structure of an example SV message is illustrated in Figure 3.3.

### 3.3.3 Security Vulnerabilities

Within the IEC 61850 standard, the GOOSE protocol is used to issue tripping and blocking commands originating from protective relays in a substation. Consequently, manipulating GOOSE data can cause unwanted relay trips and opening of circuit breakers. On the other hand, the SV protocol defines the specific communication service for the exchange of sam-

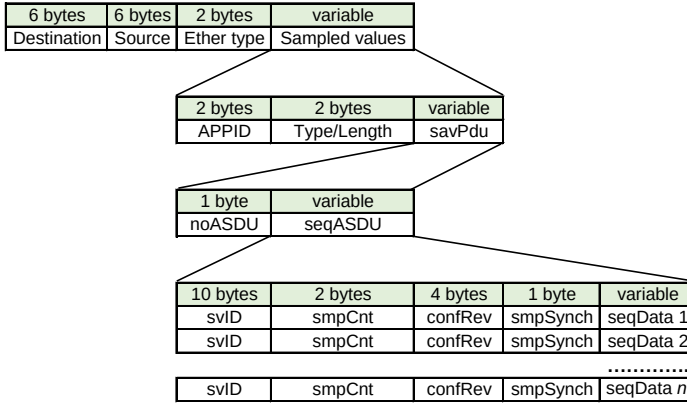


Figure 3.3: Structure of an SV protocol message.

pled values. They contain direct measurements, i.e., voltages and currents from merging units. A key point to be noted is that IEC 61850 traffic on the local operating network is not encrypted. This is to ensure strict real-time performance of protection equipment. Thus, IEC 61850-based communication is susceptible to cyber attacks [71]. Hence, the cyber attacks in the subsequent sections target the GOOSE and SV protocol messages that are encapsulated as data link (Ethernet) frames and multicast on the substation local operating network. In this chapter, IEDs refer to protection and control equipment located at the bay level and connected to the process bus. Due to the inherent structure of and processing of GOOSE and SV, the following attack types may be possible and are explained subsequently:

1. **GOOSE spoofing:** by capturing and altering a couple of fields in the GOOSE message, relays can be maliciously tripped or circuit-breakers opened.
2. **SV replay:** by capturing and replaying an SV data-stream, a denial-of-service type of attack can be inflicted on the subscribing IED.

### 3.3.4 State-of-the-Art

In related work, cyber attacks on various protections schemes, such as distance and differential protection, are discussed in [53, 67, 68]. Additionally, [75] proposes a mitigation measure for cyber attacks targeting distance protection through deep learning. However, in this research we focus on exploiting the vulnerabilities of the communication protocols used by relays in a digital substation and analysing the impact of such attacks on grid dynamics. Therefore, the particular attack model studied in this research is independent of the type of protection schemes used by the targeted protective relays. Earlier work on cyber security of power systems has demonstrated, how substation communication networks can be compromised in various ways [3, 76]. Cyber security exploits within the IEC 61850 standard have been widely studied and discussed in the literature [76, 77]. The susceptibility of the Manufacturing Messaging Service (MMS) to session hijacking, replay attacks and packet sniffing and spoofing is shown in [78]. However, within the standard,

two protocols are of major importance – GOOSE and SV. They are used to communicate critical measurements and commands within a substation in real-time. Therefore, they directly affect the protection and automation functionalities within a digital substation, making them suitable targets for cyber attacks. The various vulnerabilities and exploits of GOOSE and SV protocols are extensively discussed in [18, 71, 72, 74]. Previous work in this field has clearly established and demonstrated how IEC 61850 protocols are vulnerable to cyber attacks and may have dangerous implications on the physical power grid. However, what is found missing is the study and impact analysis of these cyber attacks on power system dynamics which this chapter and thesis broadly seeks to address. This is extremely crucial as the implications of cyber attacks on the physical power grid may be devastating, causing equipment damage or even a blackout.

### 3.4 Cyber Attack Model

A cyber attack in a digital substation is a malicious event where an adversary modifies, degrades or disables a service of at least one protection, automation or control device. This brings into question the paths and means through which cyber attacks are executed, i.e., attack vectors. To this end, physical access to the substation communication network is not always necessary. The cyber attacks can be conducted remotely by exploiting backdoors to access the local operating network, for e.g., infected station control systems or engineering workstations used for relay configurations. With the increasing adoption of IEC 61850, the traditional hard wiring of protective relays is replaced by digital communications implemented via Ethernet over fibre optics. IEC 61850 implementation does not prescribe a particular network topology, i.e., tree, star or ring. Indeed, the same physical Ethernet network could carry both the station and process bus traffic. It is also worth mentioning, a ring topology is often employed to ensure network resilience, in case of the loss of one link. In larger substations, the station bus exhibits a mixture of ring and tree topologies. At the process bus level, IEDs are typically simple measurement and actuating devices connected to the protection and control units at the bay level, which in turn interface to the station bus. Therefore, in this research, the substation communication network uses a tree topology with a focus on the cyber security of the bay level network. This is depicted in Figure 3.1. Further, IEC 61850 implements a publisher-subscriber communication mechanism for various protection schemes. In this context, the status and trip signals are communicated as GOOSE frames via the process bus between various IED at the bay level as represented in Figure 3.1. As IEC 61850 traffic is not encrypted, attackers can conduct a man-in-the-middle attack, which is the focus of this research. Such a cyber attack can be modelled in two stages as described below.

#### 3.4.1 Network Reconnaissance

The first stage of the attack model is to monitor the substation communication traffic and identify GOOSE and SV messages. The structures of a typical GOOSE and SV frame are fairly similar as shown in Figures 3.2 and 3.3. The common fields include, the physical link destination and source media access control (MAC) addresses, tag of the Virtual Local Area Network (VLAN), type header, length of the frame, and data payload. The type headers for GOOSE and SV are distinct – 0x88b8 and 0x88ba, respectively. Additionally, the actual

data payload is different. For a typical GOOSE frame, under the data payload, the data set contains the various trips commands and breaker statuses. The status and sequence number fields, i.e., *stNum* and *sqNum* are important from an operational perspective. In the processing algorithm of GOOSE messages, the sequence number is incremented continuously with every GOOSE message sent while the status number is fixed. Status number is changed by one in the case of an event, for e.g., a relay trip, and the sequence number is reset to zero. Thus, GOOSE messages with a lower status number are discarded. Similarly, the SV frame contains the *smptCnt* field, which increments with every frame transmitted. The *seqData* holds all the instantaneous phase measurements sent to the protective relays. Due to the lack of cyber security implementations, both of these protocols are susceptible to man-in-the-middle cyber attacks. Spoofed information can be supplied to the protection IEDs to trigger or inhibit protection functions. Keeping this in mind, this work seeks to formulate a generic model of a man-in-the-middle cyber attack, with a twofold objective. The first is to inject false SV data streams into the substation network. Secondly, the attack supplies spoofed GOOSE information to protective relays, causing them to trip. The first stage of the attack is completed by monitoring the network for the Ethernet source, destination, VLAN, and data payload of GOOSE and SV. Most importantly, the status number and sequence number field within the GOOSE data payload are noted. This information is used to develop an appropriate attack vector to execute the man-in-the-middle cyber attack.

### 3.4.2 Cyber Attack Execution

An attack algorithm is developed to inject spoofed GOOSE frames and replay SV frames by using information collected from the first stage. The spoofed GOOSE frames contain a modified data payload that issues a trip signal, i.e., *goosepdu*. This spoofed data frame also contains modified status and sequence number fields. By injecting this spoofed data in the process bus at a high rate, abnormal operation of protective relays is caused. Additionally, the captured SV frames are replayed. The algorithm is summarized below.

---

#### Algorithm 1: Injection of spoofed IEC 61850 traffic

---

```

Monitor network interface;
Filter packet based on type 0x88b8 (GOOSE);
Filter packet based on type 0x88ba (SV);
Capture filtered packets as  $p_{cap}$  ;
i= 0, n= number of  $p_{cap}$  ;
src = source MAC address;
dst = destination MAC address;
while ( $i < n$ ) do
     $p_{spoof}$  = Get and modify payload of  $p_{cap}$ ;
    send packet (src, dest, VLAN,  $p_{spoof}$ );
    i++;
end

```

---

### GOOSE spoofing

Under normal operating conditions, all GOOSE messages are communicated within a pre-defined time  $T$ . The normal range for  $T$  is 100 to 5000 ms. When a substation event occurs, e.g., a trip signal, the update rate of the new GOOSE messages increases to statistically assure that the message is delivered. This event mode time  $t$  has a range of 0.5 to 5 ms. Also, the status number is incremented and sequence number is reset. As previously mentioned, event mode time  $t$  of a GOOSE frame during a substation event is between 0.5 to 5 ms. This is much lower than regular operation time  $T$ . Therefore, the cyber attack may be successful if the spoofed GOOSE frames containing the malicious trip signals are sent at a higher rate in comparison to the event rate, i.e.,  $t_{attack} \ll t$ , wherein  $t < T$ . This can be observed in Figure 3.4. The IED receiving these spoofed GOOSE frames has no other option than to react, as it contains the correct source MAC address, status, and sequence number. Thus, the subscribing IED is tricked into believing a substation event has taken place. This results in an undesirable protection operation.

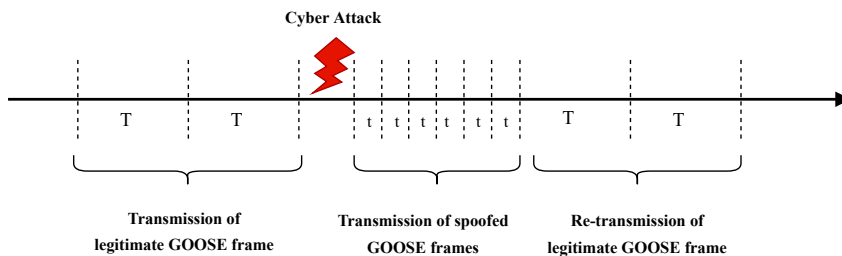


Figure 3.4: Attack model to target GOOSE data frames.

### SV Replay

There exist mechanisms in IEDs to detect voltage transformer failures. It is common for the Miniature Circuit Breaker (MCB) of a voltage transformer to trip. In that case, the measured voltage is zero and IED blocks all distance protection functions. Therefore, for a cyber attack that manipulates sampled values, changing the voltage to zero might not be sufficient to make distance protection trip. However, it might be sufficient to block the protection functions of the IED such that it fails to operate during an actual fault. The cyber attack on the SV protocol in this chapter focuses on inhibiting the protection functionality of the targeted relay. The network traffic is captured and filtered with key type of SV, i.e., 0x88ba. The rate of typical SV traffic is 80 samples/cycle. In the attack conducted in this chapter, for each captured frame, the value of measurements sent to the IED is specifically modified, which is part of Application Specific Data Unit (ASDU). The attack is carried out by spoofing the identity of the legitimate SV data stream provider (Real-Time Digital Simulator (RTDS) in this case), using the information collected from stage one. Next, we replay the spoofed frames that are completely identical to the actual SV stream, except the modified ASDU part. This modified ASDU contains spoofed data, e.g., constant data stream of zero volts, or previously observed SV data stream. This essentially creates two data streams of measurements for the IED, one with actual values from the merging unit and the other with spoofed frames. These two sets of values are unexpected

for the IED. Hence, it gets blocked from further operations. The time required for the entire process from capture, modification, and spoofed data transmission is sufficient to conduct the cyber attack, as it is carried out over two stages. Traffic is captured and analysed in stage one. Stage two only focuses on the transmission of spoofed frames to the IED.

Now, when a short-circuit occurs, the IED fails to act, as it is blocked. This causes a delay in fault clearance and may set off a chain of cascading events. With the protection device being blocked, it causes other relays in the system to trip and leads to power swing situations. Consequently, out of step conditions may result, causing generators to trip. The final result of such an attack is a blackout. This type of attack can be considered as a ‘sleeper cell’ in the substation that will present itself at a critical moment when protection needs to operate. It is interesting to note that, manipulation of the voltage/current SV measurements can create over-voltage/over-current conditions that can result in malicious tripping of the subscribing IED. However, for such an advanced SV attack, the SV traffic should come only from the attacker and the legitimate SV traffic to the IED must somehow be rerouted. Else, the IED might get blocked from further operations due to multiple concurrent input SV streams.

### 3.5 Cyber Attack Proof-of-Concept

#### 3.5.1 GOOSE Spoofing

Table 3.1 depicts the successful manipulation of GOOSE data frames, that are processed by the subscribing IED. Column 1 shows the legitimate data frames published by the physical IED to the subscriber. The false value of the Boolean field refers to the current trip status of the IED, i.e., keep the circuit breaker closed. After carefully monitoring the network, a stream of spoofed data frames is then injected at a very high rate as described previously. This causes the subscribing IED to act upon them and open the associated circuit breaker contacts. By simply altering one Boolean bit from false to true along with the status and sequence number fields, an attacker can wreak havoc on the physical power grid, as explained subsequently in this chapter. It is interesting to note, the timestamp of the spoofed data frame is wrong as shown in the table. Yet, the subscribing IED is forced to act upon these false trip signals due to the higher status number field, i.e., stNum is set to 99.

Table 3.1: Spoofing of GOOSE data frame.

| Normal operation GOOSE frame            | Spoofed GOOSE frame                     |
|-----------------------------------------|-----------------------------------------|
| gocbRef: P446_SVSystem/LLN0\$GO\$gcb01  | gocbRef: P446_SVSystem/LLN0\$GO\$gcb01  |
| timeAllowedtoLive: 2001                 | timeAllowedtoLive: 5                    |
| t: June 06, 2024 10:42:25.531999945 UTC | t: June 06, 2024 11:04:09.076999962 UTC |
| stNum: 95                               | stNum: 99                               |
| sqNum: 80850                            | sqNum: 0                                |
| numDatSetEntries: 10                    | numDatSetEntries: 10                    |
| allData: 10 items                       | allData: 10 items                       |
| Data: boolean (3)                       | Data: boolean (3)                       |
| boolean: False                          | boolean: True                           |

### 3.5.2 Hardware-in-the-Loop Setup

The hardware-in-the-loop setup used to carry out the cyber attack investigations is shown in Figure 3.5. IED 1 is fully IEC 61850 compliant, meaning, the relay has the capability for GOOSE messaging and uses SV for measurements. On the basis of the received SV input, it calculates fault condition and trip status, which is then communicated through GOOSE. IEDs 2 and 3 are partially IEC 61850 compliant. They are hardwired and receive analogue signals from RTDS through power amplifiers. The remaining relays are modelled and simulated on the RTDS. It is to be noted, all the physical IEDs used in this chapter use GOOSE messaging for critical substation communication, i.e., trip and block commands through switched Ethernet. This is keeping in line with the concept of a digital substation that employs IEC 61850. As shown, the relay data links are connected to a network switch which also has a connection to RTDS GTNET 2x card. The card is interfaced to the RTDS through an internal optic fibre connection. The card publishes sampled values to IED 1 and acts as a subscriber to the GOOSE messages from IEDs 1, 2 and 3.

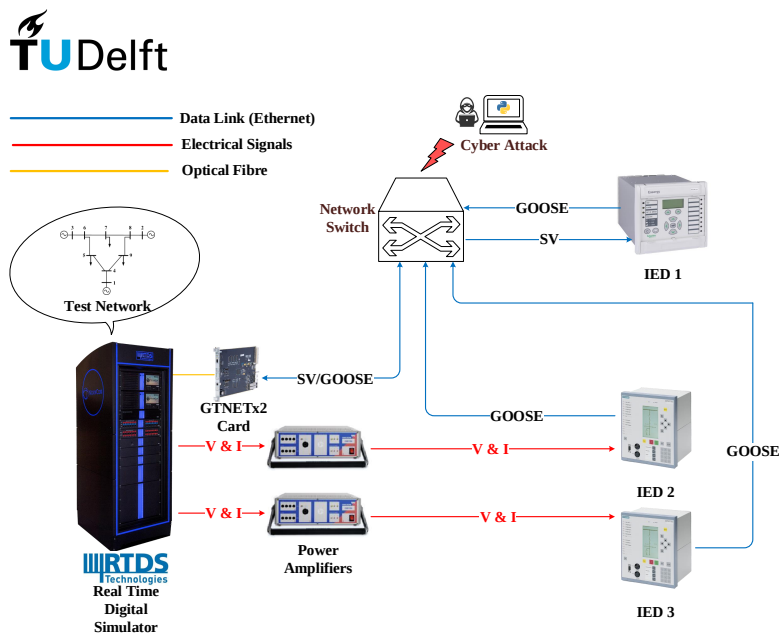


Figure 3.5: HIL cyber-physical experimental framework to analyse impact of cyber attacks on the power grid.

The proposed cyber attack model in this chapter is generic and can be carried out in two stages using a wide range of tools. We use a well-known communication network tool, i.e., Wireshark, to carry out stage one, i.e., network reconnaissance. Wireshark is run on a separate host machine, which is connected to the network switch. The network interface of this host machine is set to 'promiscuous' mode in Wireshark. This enables all the network traffic through the switch to be monitored and inspected on the host machine. The data collected from this stage is used in a python script, based on the Scapy networking library. Scapy is a packet manipulation tool for computer networks that en-

ables the crafting of spoofed data packets/frames. With access to the network switch, the script executes the man-in-the-middle cyber attack by injecting spoofed SV and GOOSE data streams directly into the substation communication network. The spoofed SV data streams cause the blocking of protection equipment. This prevents its normal operation during faults. On the other hand, the spoofed GOOSE frames compromise multiple IEDs, causing them to trip and open circuit breakers.

As previously mentioned, IEC 61850 employs a publisher-subscriber mechanism. Under this mechanism, GOOSE and SV messages are multicast using Ethernet over the process bus. This means, one IED publishes GOOSE messages to the process bus, while other IEDs only receive messages belonging to the destination address group they are configured to subscribe to, rather than all messages. Similarly, an IED is configured to subscribe to SV measurements only from a certain merging unit publishing to the process bus. In this research, the substation process bus is represented by the network switch shown in Figure 3.5. Thus, all GOOSE and SV messages are published and subscribed through the switch. To enable flexibility of connected devices, the switch is set to broadcast to all available ports, i.e., it sends packets to all connected nodes in a single broadcast domain. This is because it is not configured in secure mode. To enable this mode, flow control rules and restrictions need to be configured, which affect the flexibility and scalability of the network. Therefore, a potential cyber attacker can monitor critical substation communication traffic by gaining access to the switch and conduct packet sniffing. Moreover, the attacker can then inject spoofed packets into the network, through the switch. This forms the basis for the cyber attacks in this work.

Two power system models are simulated on the RTDS, as shown in Figure 3.6 and described below:

- 5-bus test system:** this simulated power system on RTDS has a nominal voltage level of 400 kV and frequency of 50 Hz. The biggest load centre is located at bus 4, with a total demand of 1000 MW. The system has three generation units providing 415 MW of the total load of 1500 MW. The excess load is supplied from the grid equivalent at bus 13. The single line diagram of the simulated system is shown in Figure 3.6a. Bus 4 implements an under-voltage load shedding scheme to maintain system stability in case of under-voltages or faults. UVLS is set up according to sheds load in 5% increments of the total load demand with time delays of 4 to 10 s. In addition to this, transmission line 1-2 employs an overload protection scheme. For simplification, the overload protection has been modelled with a threshold of 1.1 p.u of the nominal line current and a time delay of 7s. The targeted IEDs are highlighted in the figure, i.e., IEDs 1 and 2. IED 1 is fully IEC 61850 compliant, meaning the relay has the capability for GOOSE messaging and uses SV for measurements. IEDs 2 and 3 are partially IEC 61850 compliant. They are hardwired and receive analogue signals from RTDS through power amplifiers. Tripping commands, however, are sent as GOOSE messages.
- IEEE 9-bus test system:** the second test-system considered is the benchmark IEEE 9-bus test system. As depicted in Figure 3.6b, IEDs 1 to 3 are interfaced via Hardware-in-the-Loop at lines 8-9 and 6-9, respectively.

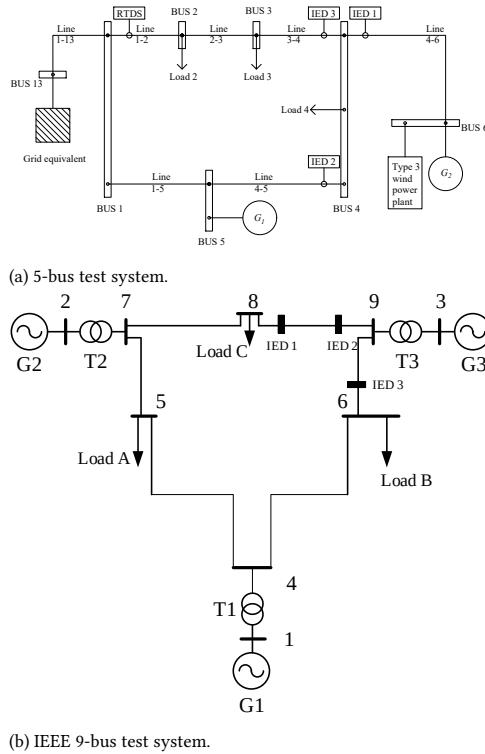


Figure 3.6: Test systems modelled and studied for cyber attack impact analysis.

## 3.6 Impact on Power System

This section discusses the impact of the aforementioned cyber attacks on the power system with respect to dynamic stability and cascading failures/outages.

### 3.6.1 Impact of GOOSE spoofing on 5-Bus Test System

#### Single attack

In the first cyber attack, only one IED's tripping command is compromised. This IED is located at bus 4 on transmission line 4-6. The attack results in a spoofed trip signal sent to RTDS by the attacker posing as the publishing IED. Consequently, this causes the circuit breaker contact of line 4-6 to open, as seen in Figure 3.7a. Due to this line disconnection, about 220 MW of generation is lost. Hence, the voltage at bus 4 drops below the nominal threshold of 0.92 p.u., as shown in Figure 3.7c. In order to restore the voltage back to acceptable levels, two steps of load-shedding is activated. This results in 100 MW of load shed due to the attack as depicted in Figure 3.7b. When analysing the frequency variation in Figure 3.7d, it is seen that the frequency of the system drops below 49.88 Hz for a short amount of time. This is due to the disconnection of the wind power plant and one of the synchronous generators, which amount to about 10% of the total generation of the system. The power deficit is accounted by the external grid. In the latter stages, frequency rises

by about 20 mHz when each step of load shedding is activated. Overall, the power system remains stable after the cyber attack on a single IED. Hence, in order to cause any sort of major damage to the power grid, a potential attacker needs to know the precise network topology and IEDs to target in the system. As per most national grid codes, it is crucial that the  $N - 1$  criterion is always satisfied. Thus, compromising only one IED may not adversely affect the power system stability.

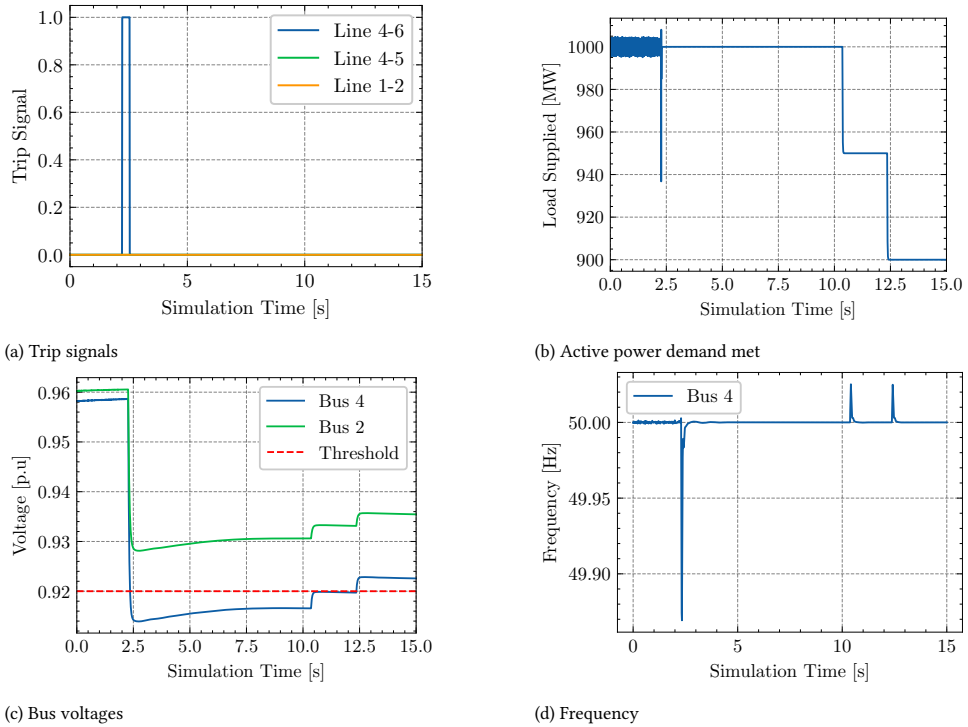


Figure 3.7: Impact of cyber attack on one IED.

### Coordinated attack

The second attack studied in this chapter is a coordinated cyber attack that targets two IEDs, i.e., IED 1 and 2. To this end, two tripping signals are compromised by a spoofing attack that results in two lines being disconnected from bus 4, i.e., 4-5 and 4-6. The tripping signals due to the attack are shown in Figure 3.8a. The overload protection causes line 1-2 to trip at 10 s simulation time. The resulting response of the power system to the attack is observed in Figure 3.8c and Figure 3.8b. Immediately post the cyber attack, the voltage in substation drops below the acceptable nominal threshold of 0.92 p.u., as observed in Figure 3.8c. Furthermore, around 8 seconds after the attack, load is shed in order to restore voltage. However, a few seconds after this around 10s, the load supplied, voltage, and frequency drop to zero because of the tripping of line 1-2. Thus, the cyber attack results in a blackout.

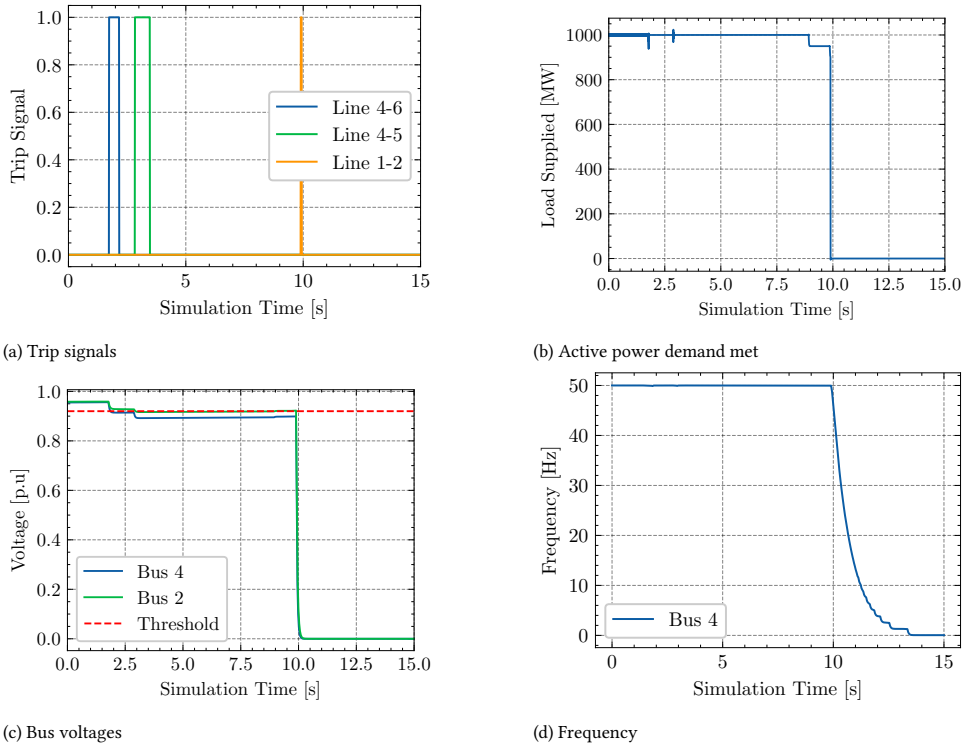


Figure 3.8: Impact of cyber attack on multiple IEDs.

### 3.6.2 Impact of GOOSE Attack on 9-bus Test System

The attack involves the malicious opening of circuit breakers in the substation at bus 7 shown in Figure 3.6b. This attack sends spoofed GOOSE data streams to three compromised IEDs in the substation. As a result of the attack, G2 and lines 7-5 and 7-8 are disconnected. The frequency drops below admissible limits as shown in Figure 3.9. This causes under frequency load shedding to take place around 5s simulation time. After three steps of load shedding, at approximately 7.5s, the system frequency starts to recover. It eventually settles to a value lesser than the nominal frequency of 60 Hz. Thus, the cyber attack results in a load shed of 90 MW, which is equivalent to a partial blackout.

### 3.6.3 Impact of SV replay attack

In this attack scenario, a SV replay attack is launched on IED 1, resulting in a denial-of-service of its protection functions. During normal operation, in the case of a fault on the transmission line 8-9, at bus 9, the fault is cleared in  $\approx 80$  ms. However, with IED 1 being blocked, the fault is not cleared on time. As a result, IED 2 trips line 8-9 first, followed by an out of step protection trip on G1, switching the generator off from the network, as seen in Figure 3.10a. The fault is then cleared by the second zone of distance protection of IED 3 located on line 6-9, which acts as a backup for blocked IED 2. Now, the system

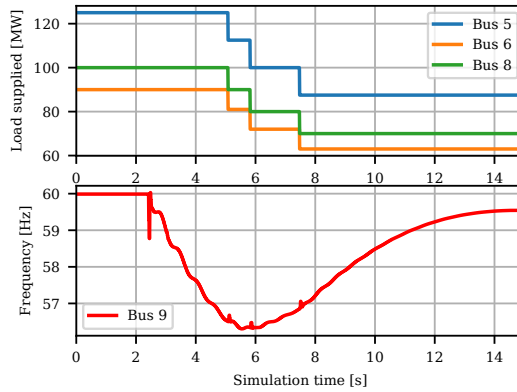
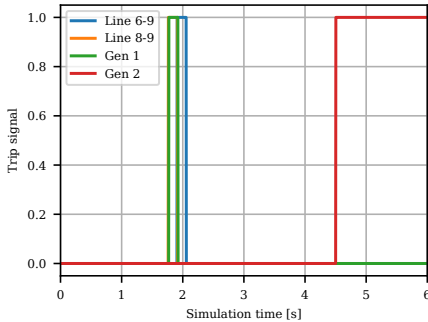
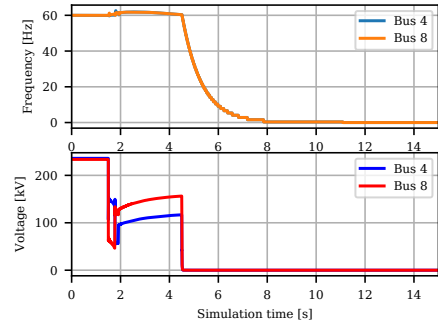


Figure 3.9: Impact of GOOSE cyber attack on 9-bus test system.

is extremely unstable and the only remaining generator, i.e., G2, cannot supply all loads. Finally, G2 is also disconnected due to an under-voltage state. Therefore, the cyber attack induces cascading failures, which lead to a blackout. Figure 3.10b shows the voltage and frequency dropping to zero. Therefore, by compromising only one IED, the cyber attack leads to a blackout.



(a) Trip signals due to cyber attack.



(b) Frequency and voltage after cyber attack.

Figure 3.10: Impact of SV cyber attack on system parameters.

### 3.7 Cyber Security of IEC 61850 GOOSE

As seen in the previous sections, cyber attacks on digital substations can have disastrous consequences on grid operations. Hence, to address these concerns, this section presents mitigation measures to prevent the types of cyber attacks described above. To this end, the IEC 62351-6:2020 standard [79] is used as the reference to implement authentication and integrity mechanisms using HMAC to secure GOOSE communications. This concept of message-authentication code is better illustrated in Figure 3.11.

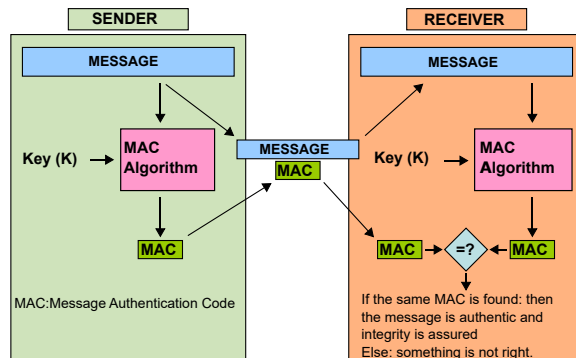


Figure 3.11: Concept of message authentication code.

### 3.7.1 IEC 62351-6 Standard

The IEC 62351-6 standard [79] is part of the IEC 62351 series, which focuses on securing communications in power systems. Specifically, IEC 62351-6 addresses security for IEC 61850 communication protocols used in substation automation, including protocols for communication between devices like circuit breakers, relays, and controllers. It ensures that messages between devices are authenticated to prevent unauthorized access and tampering. Furthermore, it recommends the usage of HMAC to ensure the integrity and authenticity of GOOSE and SV messages. For this, the recommended hash functions are SHA-256 and Advanced Encryption Standard (AES)-Galois Message Authentication Code (GMAC) [79].

### 3.7.2 Related Work

In related work, in [80], authors introduce a security scheme to defend against attacks on SV messages, which are critical for substation automation. The approach involves detecting anomalous SV messages and using encryption using Blake-2s algorithm to secure SV data transmission. Similarly, in [81], the authors present an implementation of encryption and authentication for GOOSE and SV messages, based on the earlier IEC 62351-6:2016 standard. Closer to this thesis, in [82], the authors present an architecture that ensures security for GOOSE and SV messages. The key innovation is achieving fixed low-latency encryption and message authentication under 7 microseconds, suitable for real-time substation operations. Nevertheless, the implementation is based on a custom FPGA and not real IEDs or protection devices. The concept of bump-in-the-wire security is introduced in [83] wherein a virtual solution allows to inspect and modify Ethernet traffic from legacy ICS devices. More recently, [84] introduces a novel geometric algorithm to secure IEC 61850 GOOSE through authentication and encryption. It utilizes vector coordinate shifts to achieve this. However, the proposed algorithm is new and is not recommended by IEC 62351-6:2020 [79]. Thus, it can be summarized that most existing work is based on custom implementations of protection relays/IEDs using Raspberry Pis or other embedded boards. Hence, there is a lack of actual tests/implementation with commercial relays/IEDs to secure GOOSE communications which is addressed in this chapter.

### 3.7.3 Cyber Security of GOOSE Messages

As mentioned previously, the IEC 62351-6:2020 standard recommends the usage of HMAC to ensure the integrity of GOOSE and SV messages. In this thesis, the scope of implementation is limited to GOOSE messages. To this end, the standard recommends an extension to be appended at the end of the GOOSE payload with the following fields for integrity and authentication:

- version (1 byte): current version of the extension protocol.
- timeofCurrentKey (4 bytes): UNIX timestamp of when the private key that is currently in use was generated.
- timeofnextKey (4 bytes): expected UNIX timestamp of next key to be generated. It is to be set to -1, if key is not planned to be changed.
- Init vector (2 bytes, optional): value to initialize the hash algorithm.
- keyID (4 bytes): unique ID of the current key in use.
- MAC value (8-32 bytes): the actual message-authentication tag value.

This updated GOOSE message structure is visualized in Figure 3.12. As can be seen, the extension field is appended at the end of the goosePdu, i.e., the GOOSE payload. This extension has a maximum length of 45 bytes, depending on the hashing algorithm used. For e.g, using SHA-256, the extension would be 45 bytes, with the MAC tag being 32 bytes.

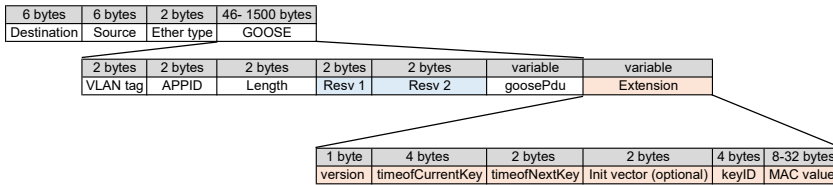


Figure 3.12: Structure of updated GOOSE message with HMAC extension.

## 3.8 HMAC Implementation

This section presents the implementation of hash-based message authentication to secure GOOSE messages. Consequently, message integrity and authenticity is ensured, thereby successfully averting the previously described spoofing and replay cyber attack scenarios.

### 3.8.1 HMAC Calculation

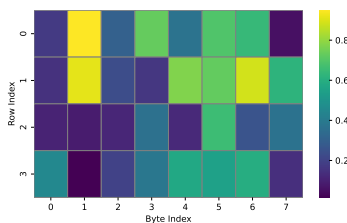
The HMAC calculation, based on the seminal work in [85] is given by the following:

$$\text{HMAC}(K, m) = H((K' \oplus o) \parallel H((K' \oplus i) \parallel m))$$

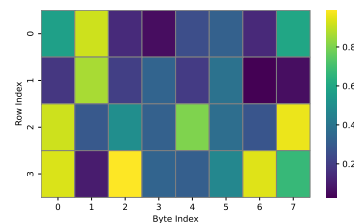
$$K' = \begin{cases} H(K) & \text{if } K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases} \quad (3.1)$$

where  $H$  is the cryptographic hash function;  $m$  is the message to be authenticated;  $K$  is the shared private key;  $K'$  is a block-sized key derived from the private key,  $K$ ; either by padding to the right with zeros up to the block size, or by hashing down to less than or equal to the block size first and then padding to the right with zeros.;  $\oplus$  represents a bitwise exclusive OR operation;  $o$  is the outer-padding; and  $i$  is the inner-padding.

In this chapter,  $H$  refers to the SHA-256 algorithm and  $m$  refers to the GOOSE payload, i.e., `goosePdu`. Since the payload contains `stNum` and `sqNum`, the resultant MAC tag of every outgoing GOOSE message is different. Furthermore, due to the inherent nature of hash algorithms being a one-way process, it is mathematically impossible to recover the original message, based on the MAC value alone [85]. Also, since the `sqNum` updates incrementally during normal operation, due to the avalanche effect of hashing, the output HMAC differs significantly. This concept is better visualized in Figure 3.13 that illustrates the differences between the MAC digests of two strings – ‘hello’ and ‘hello1’. Thereby, replay attacks can be successfully prevented as the MAC values between even successive GOOSE messages will significantly differ.



(a) SHA-256 digest heatmap for input ‘hello’.



(b) SHA-256 digest heatmap for input ‘hello1’.

Figure 3.13: SHA-256 digest heatmap visualizations to illustrate the cryptographic avalanche effect.

### 3.8.2 Architecture

The architecture of the HMAC implementation is depicted in Figure 3.14. This architecture is referred to as bump-in-the-wire. As seen, a dedicated device such as a Raspberry Pi calculates the MAC value and appends it to the GOOSE message that is then sent to the subscriber. The subscriber re-calculates a new value of the MAC code based on the received GOOSE message and shared private key. This value is then compared to the one appended in the received GOOSE message. If it matches, it means the message is authentic and originates from the correct IED and has not been tampered with. If not, there is some issue. Thus, the authenticity of the sent messages and identity of the associated publisher is clearly verified. As a result, the spoofing and replay attacks described in Section 3.4 are mitigated. The HMAC is implemented in Python 3.10 and C++ using the `hashlib`<sup>1</sup> library for the HMAC calculation and `Scapy`<sup>2</sup> for packet manipulation. The entire workflow is summarized in Algorithm 2.

<sup>1</sup><https://docs.python.org/3/library/hashlib.html>

<sup>2</sup><https://scapy.readthedocs.io/en/latest/index.html>

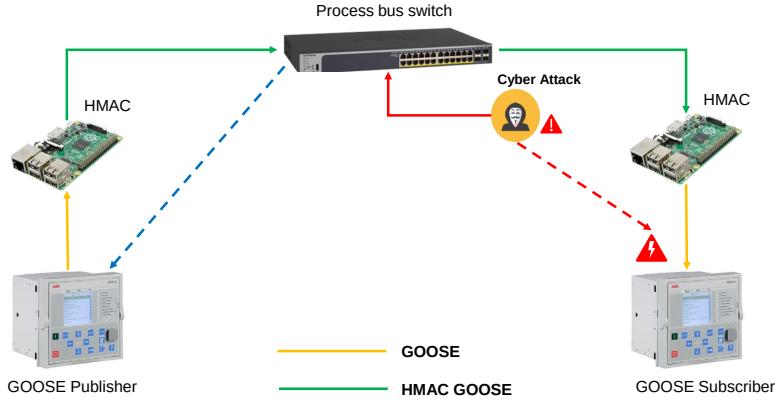


Figure 3.14: HMAC implementation architecture

**Algorithm 2: GOOSE message modification with HMAC**

**Input:** GOOSE messages, network interface, target MAC, publisher MAC, private key

**Output:** Modified GOOSE frames with HMAC tag

**Initialization:** Define network interface, target MAC, publisher MAC, and shared secret key;

**while** *Receiving GOOSE frame* **do**

    Extract GOOSE data from the frame;  
    Identify end of APDU field;  
    Calculate HMAC using shared secret key;  
    Append HMAC to GOOSE data;  
    Construct new Ethernet frame with modified GOOSE data;  
    Send modified frame to the publisher multicast MAC address;

**end**

## 3.9 Results of HMAC Implementation

### 3.9.1 GOOSE Message with HMAC Extension

Table 3.2 illustrates the comparison of GOOSE messages with and without HMAC using Wireshark packet captures. The GOOSE message payload, i.e., *goosePdu*, based on Figure 3.2 is shown in the table. As seen, without HMAC, the GOOSE part of the message has a total length of 145 bytes and along with the header of 14 bytes, the total message length is 159 bytes. Furthermore, the reserved 1 field is set to 0, since no HMAC has been implemented. On the other hand, column three depicts the modified GOOSE message with the HMAC extension. As can be observed, due to the extension, the length of the total message increases by 45 bytes, as is reflected by the updated Reserved 1 field. The MAC tag alone has a length of 32 bytes, since SHA-256 is used as the hash algorithm.

On the subscriber side, upon receiving the modified GOOSE message with the HMAC,

Table 3.2: Comparison of GOOSE messages with and without HMAC extension.

| Field                                 | GOOSE without HMAC                  | GOOSE with HMAC                                                  |
|---------------------------------------|-------------------------------------|------------------------------------------------------------------|
| APPID                                 | 0x0001 (1)                          | 0x0001 (1)                                                       |
| Length                                | 145                                 | 190                                                              |
| Reserved 1                            | 0x0000 (0)                          | 0x002d (45)                                                      |
| Reserved 2                            | 0x0000 (0)                          | 0x0000 (0)                                                       |
| goosePdu                              |                                     |                                                                  |
| gocbRef                               | SIP5_BCB1/LLN0\$GO\$Control_DataSet | SIP5_BCB1/LLN0\$GO\$Control_DataSet                              |
| timeAllowedtoLive                     | 3000                                | 3000                                                             |
| datSet                                | SIP5_BCB1/LLN0\$DataSet             | SIP5_BCB1/LLN0\$DataSet                                          |
| goID                                  | SIP/CB1/LLN0/Control_DataSet        | SIP/CB1/LLN0/Control_DataSet                                     |
| t                                     | Jul 08, 2024 08:00:15.880999982 UTC | Jul 08, 2024 08:06:41.880999982 UTC                              |
| stNum                                 | 1                                   | 1                                                                |
| sqNum                                 | 4123148                             | 4415499                                                          |
| simulation                            | False                               | False                                                            |
| confRev                               | 10001                               | 10001                                                            |
| ndsCom                                | False                               | False                                                            |
| numDatSetEntries                      | 2                                   | 2                                                                |
| allData                               | 2 items                             | 2 items                                                          |
| GOOSE HMAC extension (only with HMAC) |                                     |                                                                  |
| Version                               | -                                   | 1                                                                |
| Time of Current Key                   | -                                   | 1720426001                                                       |
| Time of Next Key                      | -                                   | -1                                                               |
| Key ID                                | -                                   | 1                                                                |
| MAC Tag                               | -                                   | 77aefb710886c617f7acb1751b5999d454e3c01f5856775ac4689e7b2c01a86b |

the subscriber device calculates the HMAC tag using Equation (3.1) based on the received GOOSE payload  $m$  and private key  $K$ . It then compares this with the extracted MAC tag from the extension field. If it matches, the GOOSE message is forwarded to the subscribing IED. This is illustrated through the terminal snippet, shown in Figure 3.15.

```
Sniffing on ens19 for GOOSE frames from b4:b1:5a:05:30:61...
APDU data: b'6181868021534950355f424342312f4c4c4e3024474f24436f6e74726f6c5f4461746153657481020bb88216534950355f424342312f4c4c4e3024446174615106472be189372a8501018603438d15870100880227118901008a0102ab088301008403030000'
Extracted HMAC: b'852d8f6de7251cf5cd75ed7282dc52f0ea7e04151b4103c09bd11f5c99086f5a'
Calculated HMAC: b'852d8f6de7251cf5cd75ed7282dc52f0ea7e04151b4103c09bd11f5c99086f5a'
HMAC verification succeeded.
HMAC verification time: 0.000387 seconds
```

Figure 3.15: HMAC verification by subscriber.

### 3.9.2 Performance Evaluation

This subsection provides a statistical evaluation of the latency associated with the HMAC bump-in-the-wire application. The total latency is determined by assessing the delays in three key components, i.e., the packet processing time for both the HMAC publisher and subscriber and the network communication latency. By analyzing these components, the evaluation shows the overall time latency incurred due to the proposed HMAC implementation. The analysis is performed based on experiments and data collected over a period of 24 hours (1 day).

Figure 3.16a illustrates the probability distribution of latency on the publisher side. As observed, the median latency for the publisher is 0.30 milliseconds, with a standard deviation of 0.03. Similarly, Figure 3.16b depicts the probability distribution of latency on the subscriber side, wherein the median latency is measured to be 0.45 milliseconds, with a standard deviation of 0.03. Additionally, we also consider the network latency between the publisher and the subscriber as shown in Figure 3.16c. In this case, the probability distribution of network latency has a median value of 0.35 milliseconds with a standard deviation of 0.02. Furthermore, we also consider the processing latency of the IED as shown in Figure 3.16d with a median value of 0.72 milliseconds and standard deviation of 0.09. Meanwhile, the processing latency of the RTDS GTNET card is 0.10 milliseconds, with a standard deviation of 0.01 as depicted in Figure 3.16e. Based on the above, the total latency  $\tau_{total}$  is calculated as follows

$$\tau_{total} = \tau_{pub} + \tau_{sub} + \tau_{net} + \tau_{IED} + \tau_{GTNET} \quad (3.2)$$

which gives total latency,  $\tau_{total} = 0.30 + 0.45 + 0.35 + 0.72 + 0.10 = 1.92$  ms.

Therefore, this average value successfully meets the standard requirement of Transfer Time class 6 (TT6) with a maximum latency of 3 milliseconds, as specified in the IEC 61850-5:2013 standard. In the experiments, we also consider the worst-case scenario latency based on the maximum latency from all parts. The largest possible latency based on the total largest latency from all parts is 2.663 milliseconds. Even in this case, the latency still meets the requirement of TT6 maximum latency. Hence, based on the experiments, the proposed solution is suitable for enhancing the cyber security of GOOSE messages within digital substations.

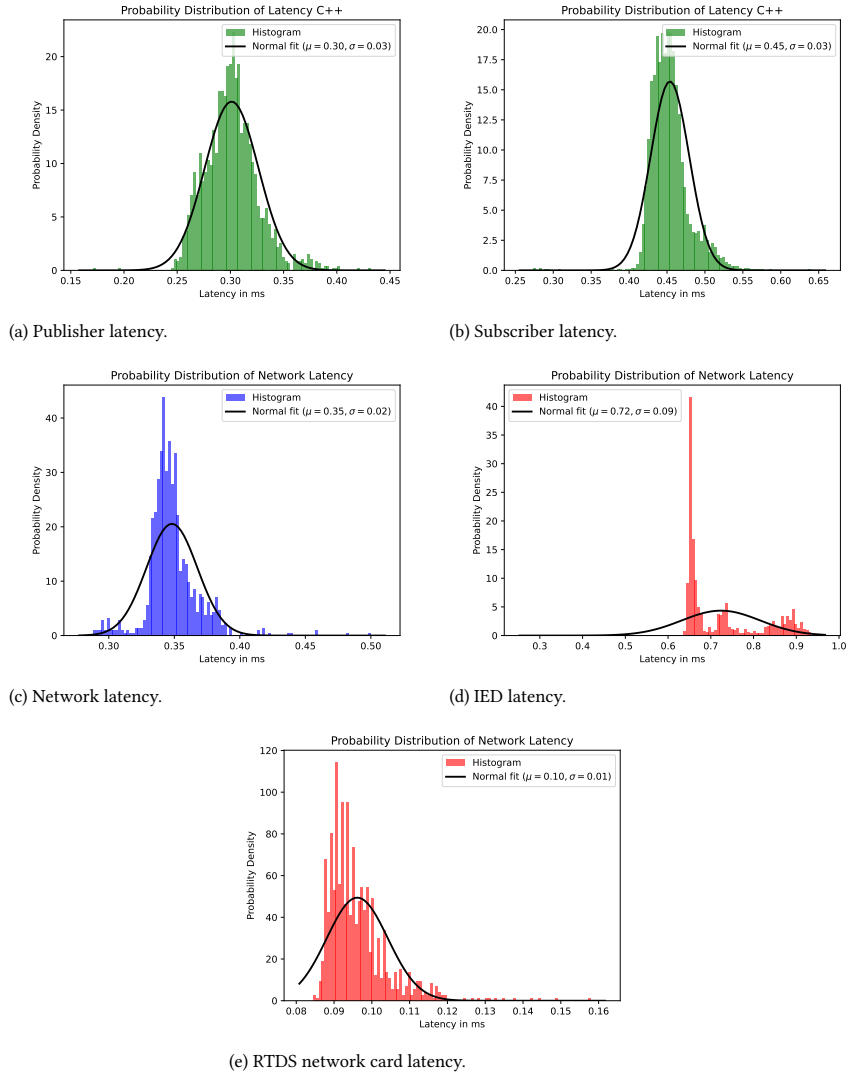


Figure 3.16: Statistical analysis of latencies for HMAC application.

### 3.10 Concluding Remarks

The key findings of this chapter and related answers to research questions are summarized as follows.

#### RQ1.1 How to show quantitatively that cyber attacks can cause cascading failures?

This chapter presented the cyber security implications of not securing IEC 61850 standard used for power substation automation and protection. Man-in-the-Middle cyber attacks are demonstrated to achieve protection relay blocking and malicious opening of circuit breakers in the power system. The attacks cause cascading failures, leading to a partial or complete blackout. This is validated using the proposed HIL experimental framework consisting of commercial relays and RTDS.

#### RQ2.1 How to secure GOOSE messages in digital substations to mitigate cyber attacks?

To mitigate cyber threats within digital substations, the IEC 62351-6 standard proposes an additional field to the GOOSE and SV data payloads for security-relevant information. The standard recommends using hash algorithms such as SHA-256 to generate a HMAC for the GOOSE and SV messages to check the integrity and ensure authenticity of the messages. This can ensure cyber security, while adhering to the strict real-time protection requirements of  $< 4\text{ms}$ . Results from this chapter demonstrated that usage of HMAC can mitigate the threat of spoofing and replay attacks targeting IEC 61850 GOOSE. Nevertheless, this necessitates a key management infrastructure within the digital substation to be updated and maintained by utilities. Consequently, this security mechanism is not supported by most vendors and has therefore not yet gained widespread use within the industry.

## 4

# Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks

4

*Cascading failures in power systems are extremely rare occurrences caused by a combination of multiple, low probability events. The looming threat of cyber attacks on power grids, however, may result in unprecedented large-scale cascading failures, leading to a blackout. Therefore, new analysis methods are needed to study such cyber-induced phenomena. In this chapter, we propose a data-driven method for dynamical analysis of power system cascading failures caused by cyber attacks. We provide experimental proof on how attacks may accelerate the cascading failure mechanism, in comparison to historically observed blackouts. Using a dynamic power grid model, consisting of multiple, coordinated protection schemes, we define and analyse the point of no return in a cascading failure sequence by applying the Hilbert-Huang transform for time-frequency analysis. Numerical results indicate, cyber attacks may accelerate cascading failures at least by a factor of 3x. This is due to the excitation and non-damping of multiple frequency modes greater than 1 Hz in a short time span. The proposed method is tested using time domain simulations conducted through a modified IEEE 39-bus test system, which can simulate cascading outages using coordinated protection schemes.*

## 4.1 Motivation

Cyber attacks on power grids are a real modern-day threat with considerable ramifications. They are no longer a figment of imagination, considering recent real-world events. The most famous and well-known examples of cyber attacks targeting power grids are the attacks in Ukraine in 2015 and 2016. Cyber attacks on power systems may instigate multiple, unprecedented excitation modes, and lead to an accelerated point of no return in the cascading failure sequence. Hence, the impact of a cyber attack on power system dynamics can be fundamentally different from the consequences of physical faults or contingencies. This can lead to unprecedented  $N - k$  contingencies. Consequently, there is a compelling need for the development of newer analysis methods that are specifically tailored to the distinctive characteristics of cyber attacks on power systems. Furthermore, as described earlier, one of the key limitations of most existing methods is the analyses based on power flows or network topology. Thereby, such studies do not take dynamical behaviour of the power system into account. This results in an incomplete view of the underlying mechanisms that govern power system cascading failures. Hence, to overcome these drawbacks, in this chapter, we analytically show how cyber attacks can cause cascading failures and blackouts and lead to a quicker point of no return. This is achieved through detailed modelling and simulation of power system dynamics and multiple, coordinated protection schemes for lines, generators, and loads. It allows us to analyse in time domain the entire sequence of cascading events, i.e., protection trips of transmission lines and generators

## 4.2 State-of-the-Art

Analysis of power system cascading failures and blackouts is extensively documented in the literature [50, 86, 87]. Most existing work focuses on steady-state methods, such as DC [5, 8, 88] and AC power flow models [89] that capture overloading conditions and voltage violations. Given the complexity of the electrical power system, however, such methods only provide a partial view of the cascading failure mechanism. Furthermore, a major drawback of such methods is the inability to study non-linear and dynamic phenomena that have been observed in real-world cascading failures. For example, loss of synchronism and voltage collapse. Other techniques include statistical methods based on historical data [5] and graph theory models to describe the generalised behaviour of cascading effects [7, 90]. While offering broad mathematical and analytical insights, however, both methods are limited in capturing the power system physics. In other related work, extensive research has been conducted with dynamic grid models to simulate system instability caused by large disturbances [10, 11]. Such numerical studies, however, consider only a particular type of instability phenomena and just highlight when the power system becomes unstable, e.g., rotor swings and oscillations. Major cascading outages consist of two distinct phases [12]. The slow phase is in the order of a few minutes to hours, while the fast phase occurs in the order of a few milliseconds to seconds. In the latter, various non-linear and dynamic phenomena dominate, e.g., transient, frequency, and voltage stability. Hence, research into dynamic modelling and dynamic simulations of cascading failures has gained increased attention.

The study and analysis of cascading failures due to cyber attacks is a relatively emer-

gent topic of research, in the wake of the cyber attacks in Ukraine in 2015 and 2016. The role and impact of cyber attacks on power system stability and cascading failures is discussed in [91]. The authors present a screening method for the initiating cyber events and perform dynamic simulations for the identified critical study cases. This study, however, stops when the power system is deemed unstable, thereby ignoring the sequence of cascading events. In other related work, [92] presents a cascading failure vulnerability analysis by studying the interdependence between cyber and physical layers. However, this work does not analyze the cascading failure mechanism itself.

Closer to this chapter is the Markov-chain based dynamical probabilistic model developed in [93]. This model partially captures the dynamics of cascading failures in the power grid but does not analyse the point of no return or global instability, which is the focus of our work. Multiple recent studies have been conducted to model and analyse cascading failures in smart grids based on power flow analysis [30, 55]. Such studies analyse the impact of line overloads or loss of equipment, but do not capture the dynamics of the fast-cascading failure mechanism. Hence, it can be summed up that limited work has been carried out in employing detailed dynamic RMS models with comprehensive and coordinated protection schemes for analysis of power system cascading failures caused by cyber attacks. The work in [28] serves as the foundation of this work. The authors provide a comprehensive analysis of major blackouts, with a particular emphasis on the cascading failure mechanism. This work delves into the intricate dynamics and root causes of cascading failures, offering invaluable insights into the factors that trigger them and the subsequent chain reactions that lead to blackouts. Most importantly, the authors coined the term, point of no return. This signified a point of global instability beyond which power system collapse was imminent. However, the authors did not formalize nor quantify it which is the focus of our work.

## 4.3 Cyber-Physical Attacks on Power Grids

Various types of cyber attacks on power grids are already well reported in literature. In this chapter, we consider attack vectors with maximum impact and scenarios that can severely affect system dynamics, thereby leading to cascading failures and a blackout.

### 4.3.1 Spoofing Attacks

These cyber attacks target the setpoints of control devices and mechanisms of generators, e.g., governors for Load Frequency Control (LFC) and AVR. This is also applicable to controllers for power electronics interfaced generation, such as solar or wind-farms. The attacks aim to send malicious control signals that result in equipment or component malfunctions. A resonance cyber attack targeting LFC of generators is discussed in [56]. In this type of attack, an adversary modifies the input signals to generator governors based on a resonance source, e.g., ROCOF. This results in a negative feedback on load frequency control, such that the targeted generator loses stability, resulting in unexpected loss of generation. Similarly, in the event of over or under excitation AVRs of generators can trip for safety reasons. This can cause voltage stability issues and lead to a voltage collapse. Thereby, spoofing attacks can initiate or worsen an ongoing cascading failure process.

### 4.3.2 Switching Attacks

These types of cyber attacks aim to maliciously open multiple circuit breakers to impact power system operation. Let us consider a power system with  $n$  circuit breakers. We assume an attacker has access to  $m$  of these circuit breakers such that  $m \subseteq (n)$ . This is possible through communication network exploits or digital substation based attack vectors. Then, the attack vector for switching is given by the following relation where  $sw$  corresponds to a binary variable indicating connection or disconnection.

$$SW = [sw_1, sw_2 \dots sw_m]^T = [0, 0, \dots 0]^T \quad (4.1)$$

Thereby, the attacker can disconnect multiple transmission lines and other power system components. For instance, the unexpected loss of lines causes equipment to be disconnected as well as system parameters like voltage and frequency to exceed limits. As demonstrated during the 2015 cyber attack in Ukraine, lines can be put out of service by gaining unauthorized access to the substation automation systems and simultaneously opening multiple circuit breakers. This results in overloading of parallel lines, setting off a cascade that could result in a voltage collapse. As observed in Italy and the United States-Canada in 2003, this can have a particularly catastrophic impact on the power system, leading to a blackout.

### 4.3.3 Data Integrity Attacks

FDI attacks are the most frequently discussed cyber attack on power systems in the literature. An FDI attack assumes that an attacker may gain access to knowledge about the existing configuration of the power system and alter measurements at substations. As a result, they might secretly insert arbitrary biases to some state variables. Hence, the majority of FDI attacks reported in the literature target state estimate methods and measurements to result in data integrity issues and potential line overloading or even cascading failures. Another form of data integrity attack reported in the literature targets power system protection equipment. Communication-based protection schemes are vulnerable to data integrity attacks that can manipulate the data sensed by protection relays, causing them to maliciously trip or malfunction, as described in Chapter 2. This is summarized by the following relation which highlights the spoofing of the relay pickup current:

$$I_{pickup}^* = I_{pickup} \pm \beta \quad (4.2)$$

where  $\beta$  represents the bias added as a result of the cyber attack. Such sophisticated cyber attacks can lead to malicious tripping of relays, while remaining undetected. This can have crippling consequences for power system operation as the attacks can result in unwanted opening of circuit breakers, leading to transient and/or voltage instabilities. Another possibility is a DOS attack. In this scenario, the protection equipment is inhibited or blocked from normal functioning. Hence, during a fault condition, the relay may not operate, causing other zones of protection to be activated. This can subsequently cause unwanted relay tripping, thereby triggering a chain of cascading events [94].

### 4.3.4 Cyber-Physical Attacks

Interlocking is an important safety mechanism that is commonly used in digital substations to ensure the safe operation of switch gear equipment. It involves the use of a

software-based scheme that uses IEC 61850 GOOSE to exchange information between control units in different parts of the substation. For example, in a two-busbar single breaker arrangement with two feeder bays and a coupler, as shown in Figure 4.1, the coupler and circuit breaker statuses are communicated to the feeder Bay Control Unit (BCU) to prevent the inadvertent opening of disconnects when the circuit breaker is closed. However, despite its importance, interlocking is vulnerable to cyber attacks that can compromise the system's security. In particular, attack vectors reported in the literature from Chapter 3 can allow disconnects to be operated in the feeder bays even when the circuit breakers of the feeders are closed, putting the system at risk. This can result in a bolted busbar fault and electric arc in the substation. Coupled with a denial of service attack which may inhibit protection functionality, this can cause massive system instabilities and lead to a blackout.

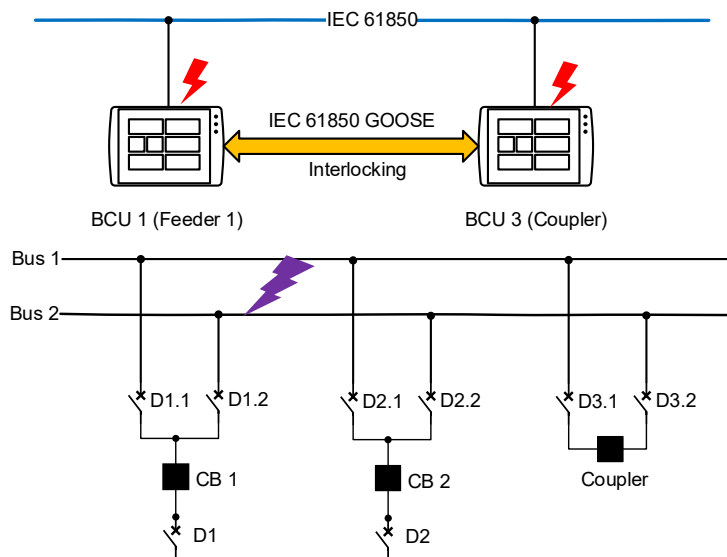


Figure 4.1: Interlocking scheme in digital substations.

## 4.4 Dynamical Analysis of Cascading Failures

### 4.4.1 Power System Dynamics

Power system dynamical behaviour is characterised by two main properties, i.e., non-linearity and non-stationarity. This makes a detailed analytical study of such behaviour complex. Hence, modern-day power system studies involve modelling the power grid and associated components as a set of differential algebraic equations to be numerically solved in the time-domain. The continuous time behaviour of the dynamical power system can be generally described by a general set of Differential Algebraic Equations (DAEs), wherein, the states and the dynamic behaviour of the power system at any time instant  $t$  is given

by three vectors  $x(t), y(t), z(t)$ , such that

$$\begin{aligned}\dot{x} &= f(x(t), y(t), z(t)) \\ g(t, x(t), y(t), z(t)) &= 0 \\ h(t, x(t), y(t), z(t)) &< 0\end{aligned}\tag{4.3}$$

$x$  represents the vector of all state variables,  $y$  represents a vector of continuous state variables with algebraic associations to all other system variables. This includes the standard power flow equations and algebraic equations for all dynamic devices such as motors, converters, condensers, etc, and  $z$  represents the vector of discrete state variables, i.e.,  $z \in [0, 1]$ . It captures the dynamics associated with discrete actions, such as protection and controls.

In this chapter, a dynamic RMS model of the power system with multiple, coordinated protection schemes is developed. If the input parameter sensed by a protection  $I_s$  exceeds a specified pickup or threshold value over a specified time period, the relay produces a trip signal to open the associated circuit breaker. A binary variable  $K_s$  determines the trip status of the relay and can be generalized by the following logic, with 1 being the trip state:

$$K_s = \begin{cases} 0, & 0 < I_s \leq I_{\text{pickup}} & t < t_{\text{lim}} \\ 1, & I_{\text{pickup}} < I_s < I_{\text{lim}} & t > t_{\text{lim}} \end{cases}\tag{4.4}$$

This logic is incorporated into the developed dynamic RMS model. Hence, it can simulate cascading failures and associated dynamic system response. With increasing system size, purely analytical studies of power grids are challenging and numerical simulations are needed. Hence, we perform time-domain simulations and use the dynamic system response for further analysis.

#### 4.4.2 Time-Frequency Analysis

To capture both non-linear and non-stationary system behaviour, we employ a modified Hilbert–Huang Transform (HHT) and study the point of no return. It is a signal processing technique for data analysis of non-linear and non-stationary processes and consists of an iterative Empirical Mode Decomposition (EMD). In this chapter, an EMD process for power systems is used to decompose an input signal, i.e., power system measurement, into a series of individual amplitude and frequency-modulated components, i.e., Intrinsic Mode Functions (IMFs) [23]. The IMFs are computed based on the sifting process. IMFs are characterised by being nearly monotonic, i.e., consisting of a single frequency component. Consequently, we apply the Hilbert transform on IMFs, which allows for a detailed analysis into the temporal modal properties of the input signals. As a result, an in-depth interpretation of non-linear and non-stationary phenomena is achieved. For a given time-series signal input,  $u(t)$ , we first compute the major IMF using EMD and then compute its Hilbert Transform (HT) as follows:

$$H[u(t)] = -\frac{1}{\pi} \lim_{\epsilon \rightarrow 0} \int_{\epsilon}^{\infty} \frac{u(t+\tau) - u(t-\tau)}{\tau} d\tau\tag{4.5}$$

Two of the known limitations of the HHT are mode mixing, i.e., close proximity of frequency components and presence of low frequency components. To overcome these limi-

tations, in this research, we apply a modified EMD procedure with an iterative-EMD technique. This technique automatically identifies the best masking signal frequencies based on the inherent dynamics of the input data signal. Based on the HT, the analytical signal of the input is computed and expressed as an exponential, i.e.,

$$u_a(t) = u(t) + jH[u(t)] \quad (4.6)$$

$$u_a(t) = Ae^{j\omega(t)} \quad (4.7)$$

Using the above, it becomes possible to calculate instantaneous parameters such as amplitude, as follows:

$$A = \sqrt{u^2(t) + H^2[u(t)]} \quad (4.8)$$

Knowledge of the instantaneous amplitude and phase information allows to estimate the instantaneous damping. This allows for a deeper stability analysis of the system. The damping is calculated as the ratio of the differential of the instantaneous amplitude to itself, i.e.,

$$\alpha(t) = -\frac{d\phi(t)}{dt} = -\frac{\dot{A}(t)}{A(t)} \quad (4.9)$$

This opens up interesting possibilities for analysis of dynamic system response, while preserving temporal properties, as explained in the subsequent subsections.

#### 4.4.3 Instantaneous Damping Correlation

The analysis of the Point of No Return (Point-of-No-Return (PNR)) in this paper is inspired by the analogy and similarities between non-linear mechanical and electrical systems. When such dynamic systems are subject to systemic failures, points of global instability may surface. For example, consider a simple example of a mass-spring system with a single degree of freedom, governed by the following differential equation:

$$m\frac{d^2x}{dt^2} + c\frac{dx}{dt} + kx = 0 \quad (4.10)$$

where,  $x$  is the system state,  $m$  is the spring mass,  $c$  is the damping coefficient, and  $k$  is the spring constant. Calculating its system and damping response is quite straightforward. More interestingly, however, this equation bears close resemblance to the well-known swing equation, governing fundamental power system dynamics:

$$\frac{d(\Delta\omega_r)}{dt} = \frac{1}{2H}(T_m - T_e - K_D\Delta\omega_r) \quad (4.11)$$

The above equation is the so called classical swing equation with two state variables – the generator rotor angle ( $\delta$ ) and angular speed ( $\omega_r$ ). This simple and elegant relation provides powerful analytical insights into grid dynamics. Inspired by the similarities between Equation (4.10) and Equation (4.11), the proposed algorithm in this work seeks to leverage the properties of instantaneous damping, to characterise and study the PNR.

Any cascading failure sequence involves loss of multiple elements, captured through the discrete relay trip events  $K_s$ . Thereby, the order and time of tripping serves as an

important input to identify and quantify PNR. The observation time window around each trip event  $K_s$  is dependent on the timing of the discrete relay actions at  $t_i$ . The proposed sliding time window  $T_i - 1$  around each discrete relay action at  $t_i$  is given by:

$$T_{i-1} = \left\{ \frac{\Delta t_{i,i-1}}{2}, \frac{\Delta t_{i,i+1}}{2} \right\} \quad (4.12)$$

Figure 4.2 summarizes the calculation of  $T \in \{T_1, T_2 \dots T_n\}$ . It captures the continuous dynamical variations occurring in the power system due to sequential relay tripping events, which indicate cascading failures. Therefore, the sliding time window  $T$  allows us to analyse the entire sequence of cascading failures.

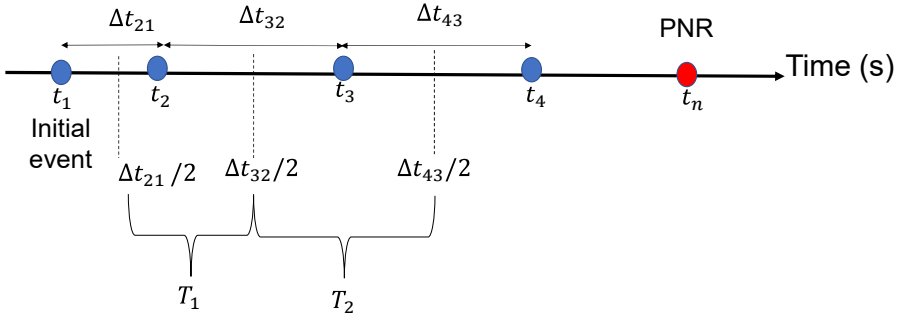


Figure 4.2: Sliding time windows for cascading failures analysis.

For each time window, we then estimate the instantaneous damping, based on Equation (4.9). Subsequently, a cross-correlation matrix  $R$  is formed, for  $n$  number of time-series signals, i.e.,

$$R = \begin{bmatrix} E[X_1 Y_1] & E[X_1 Y_2] & \dots & E[X_1 Y_n] \\ E[X_2 Y_1] & E[X_2 Y_2] & \dots & E[X_2 Y_n] \\ \vdots & \vdots & \ddots & \vdots \\ E[X_m Y_1] & E[X_m Y_2] & \dots & E[X_m Y_n] \end{bmatrix} \quad (4.13)$$

where  $E(X_i, Y_i)$  represents the correlation between the two variables, i.e.,

$$E(x, y) = \frac{1}{n} \sum_{i=1}^n (x - \mu_x)(y - \mu_y) \quad (4.14)$$

This is a measure of how two variables change with respect to each other. Hence,  $R$  contains the combination of correlations between all values of instantaneous damping and is of size  $n \times n$ . These values lie in the range  $[-1, 1]$ .

#### 4.4.4 Point of No Return and Singular Value Decomposition

SVD is a linear algebraic technique to factorise any  $n \times n$  matrix and generalize its eigen decomposition. In our case, the matrix  $R$  is symmetric, therefore, its SVD yields

$$R = USV^T \quad (4.15)$$

where  $U$  and  $V$  are distinct orthogonal matrices, and  $S$  is a sparse diagonal matrix containing the singular values of  $R$ , i.e.

$$S = \begin{bmatrix} \sigma_i & 0 & \cdots & 0 \\ 0 & \sigma_j & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n \end{bmatrix} \quad (4.16)$$

where  $\sigma_i \dots \sigma_n$  are the singular values of  $R$  in descending order, i.e.,  $\sigma_1 > \sigma_2 \dots \sigma_{n-1} > \sigma_n$ . Essentially, SVD helps to identify dimensions along which data is best preserved by the largest singular values. Hence, under nominal operations, matrix  $R$  is a zeros matrix and consequently  $\sigma_1 = 0$ . If the power system suffers a major disturbance, however, for e.g., an electrical fault, it will suffer undamped oscillations, i.e.,  $\alpha(t) \rightarrow -1$ . Subsequently, post fault, the system will reach a new equilibrium point and oscillations will be over/critically damped, i.e.,  $\alpha(t) \rightarrow 1$ . In case of an unchecked cascading sequence, however, the system will move between highly unstable operating points, reach a point of no return and collapse. Consequently, the system-wide oscillations are undamped across multiple time-windows, i.e.,  $\alpha(t) \rightarrow -1$ . As a result, we hypothesize that  $\sigma_1$  of  $R$  will drop below the theoretical threshold, i.e.,

$$\Delta\sigma = \sigma_1 t_1 - \sigma_1 t_2 \gg 0 \quad (4.17)$$

where  $t_1$  and  $t_2$  represent successive time windows (only for notation). Hence, Equation (4.17) forms the limit criterion and theoretical basis to identify the smallest/earliest point of no return and is summarised by the following algorithm. The proposed algorithm is meant to be used for post-mortem analysis and takes time occurrence of events and time-series measurements as inputs. Subsequently, it application yields an estimation of the earliest PNR value, which is non-trivial, as noted in [28].

---

**Algorithm 3:** Identification of point of no return

---

**Input:** Time window vector  $T$  and signals  $x(t)$   
 estimate sliding time window;  
**for each time window  $T$  do**  
     compute instantaneous damping  $\alpha(t)$ ;  
     form cross-correlation matrix  $R$ ;  
     calculate  $\sigma_0, \sigma_1$  using Equation (4.17);  
     obtain  $\Delta\sigma = \sigma_0 - \sigma_1$ ;  
     **if**  $\Delta\sigma > \epsilon$  **then**  
         possible PNR. Set smaller  $T$  and repeat steps 3 to 6;  
     **else**  
          $T = T_{\text{next}}$ ;  
     **end**  
**end**

---

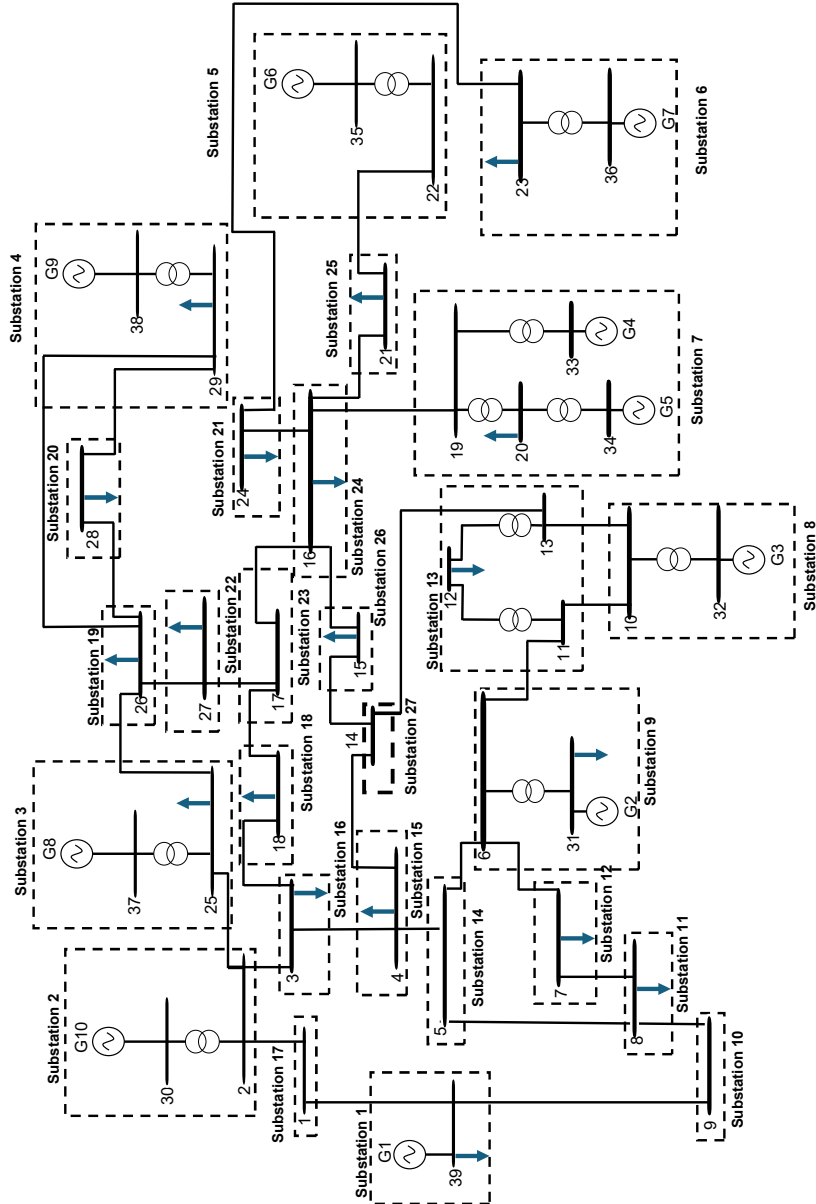


Figure 4.3: IEEE 39-bus single line diagram with 27 user-defined substations.

## 4.5 Experimental Results

In this section, we discuss a simulation case study involving cyber attacks conducted on a transmission system digital substation. The simulations are carried out on a modified IEEE-39 Bus test system simulated on DiGSILENT PowerFactory. The OT network is emulated using Mininet, based on operating-system-level virtualization. The entire emulated OT network runs on 10 virtual servers and consists of 27 user-defined substations as shown in Figure 4.3, 118 measurement devices, and over 800 data points for the entire simulated power system. SCADA device functionality within the OT network is realised through custom Python code. To analyse the impact of cascading failures, multiple coordinated protection schemes are implemented. These include interface protection for generators in the form of under/over-frequency, Rate-of-Change-of-Frequency (ROCOF), loss of synchronism, and under/over voltage. For the transmission lines, distance protection along with line overloading protection is enabled. Stress mitigation includes under frequency and under voltage load shedding.

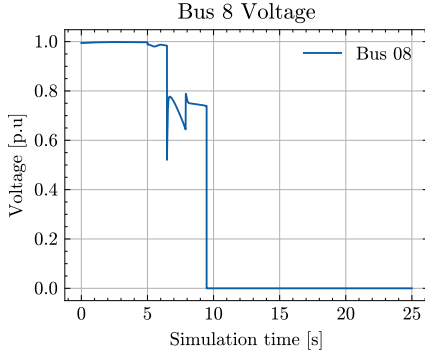
### 4.5.1 Cascading Failure Simulations

#### Cyber Attack on Substation 14

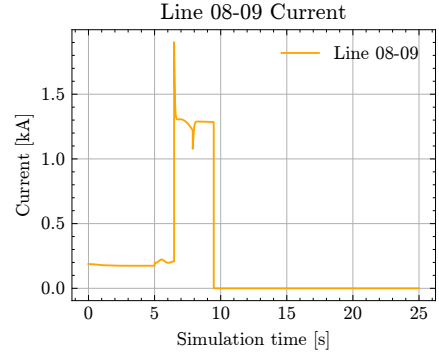
The aforementioned cyber attack results in the malicious disconnection of lines 05-06, 04-05, and 05-08, along with a DOS attack that restricts remedial actions by the system operator. Consequently, the prolonged cyber attack affects power system stability. Multiple lines are disconnected by distance relays operating on sustained under voltages and over currents. Such a phenomenon was also observed during the North American cascading failures and blackout in 2003. A critical line is tripped due to incorrect operation of zone 3 distance protection, aggravating the domino effect and leading to the spread of the cascading phenomenon, ultimately ending in a large-scale blackout. An example of such a trip is shown through Figure 4.4b for line 08-09. As a result of multiple line disconnections, generators in the system are extremely stressed and operating close to their limits. Finally, in the absence of remedial actions, generator G3 is tripped by its interface protection due to a high ROCOF condition, well exceeding the ROCOF setting of 2 Hz/s, as seen in Figure 4.4d. A similar condition leads to the loss of generator G2. Now, due to the loss of generation, system frequency starts plummeting and emergency load shedding is activated to preserve system integrity. Ultimately, the cyber attack leads to a partial blackout with 10 busbars being de-energized and a loss of load amounting to 772 MW. The cascading failure sequence is summarized in Table 4.1.

#### Cyber Attack on Substations 14 and 21

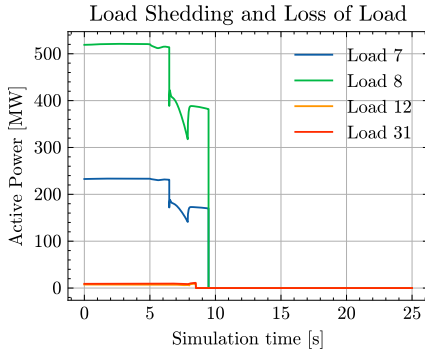
In this simulation scenario, substations 14 and 21 are targeted by cyber attacks at different time intervals. The three lines in substation are disconnected at 5, 6, and 7 seconds, respectively. This results in the overloading of neighbouring lines that eventually trip due to distance protection. As a result, generators G2 and G3 are islanded. Subsequently, both are tripped by ROCOF protection around 9.5s. Following this, substation 21 is targeted by the cyber attack and all lines within the substation are disconnected. Following this, the system experiences severe dynamic instabilities, followed by tripping of multiple generators, eventually resulting in a blackout. Three islands remain with external grid, G4 and G10 supplying load 20, 25, and 39, respectively. These phenomena are visualized



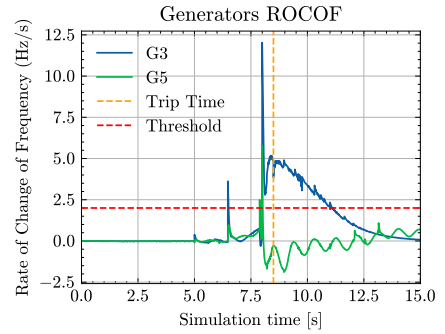
(a) Bus 8 voltage.



(b) Distance protection tripping of line 08-09.



(c) Load shedding due to cyber attack.



(d) ROCOF tripping of generators 3 and 5.

Figure 4.4: Power system dynamics and cascading failures caused by cyber attack on substation 14.

Table 4.1: Sequence of cascading failures due to cyber attack on substation 14.

| No. | Time          | Event                                                                                                               |
|-----|---------------|---------------------------------------------------------------------------------------------------------------------|
| 1.  | 0s            | Start of simulation.                                                                                                |
| 2.  | 5s            | Cyber attack on substation 14. Lines 05-06, 04-05, and 05-08 maliciously disconnected.                              |
| 3.  | 6.4s          | Distance relay trips line 06-07. Power grid is split into 2 isolated areas.                                         |
| 4.  | 7.8 to 7.9s   | Lines 10-13 and 13-14 in vicinity of attacked substation tripped by distance protection.                            |
| 5.  | 8.4s          | Generators G3 and G2 tripped due to ROCOF interface protection and disconnected. System is now heavily stressed.    |
| 6.  | 9.4s          | Line 08-09 trips on distance protection. Two areas now left unsupplied.                                             |
| 7.  | 12.0 to 12.5s | Underfrequency load shedding activated. All loads shed by 6.5%.                                                     |
| 8.  | 13.0 to 18.6s | System frequency is still below permissible limits. Underfrequency load shedding activated in steps of 5.9% and 7%. |
| 9.  | 25s           | End of simulation. Power outages with total loss of load amounting to 772 MW.                                       |

in Figure 4.5. The total loss of load amounts to nearly 4000 MW and the entire sequence of events is summarized in Table 4.2.

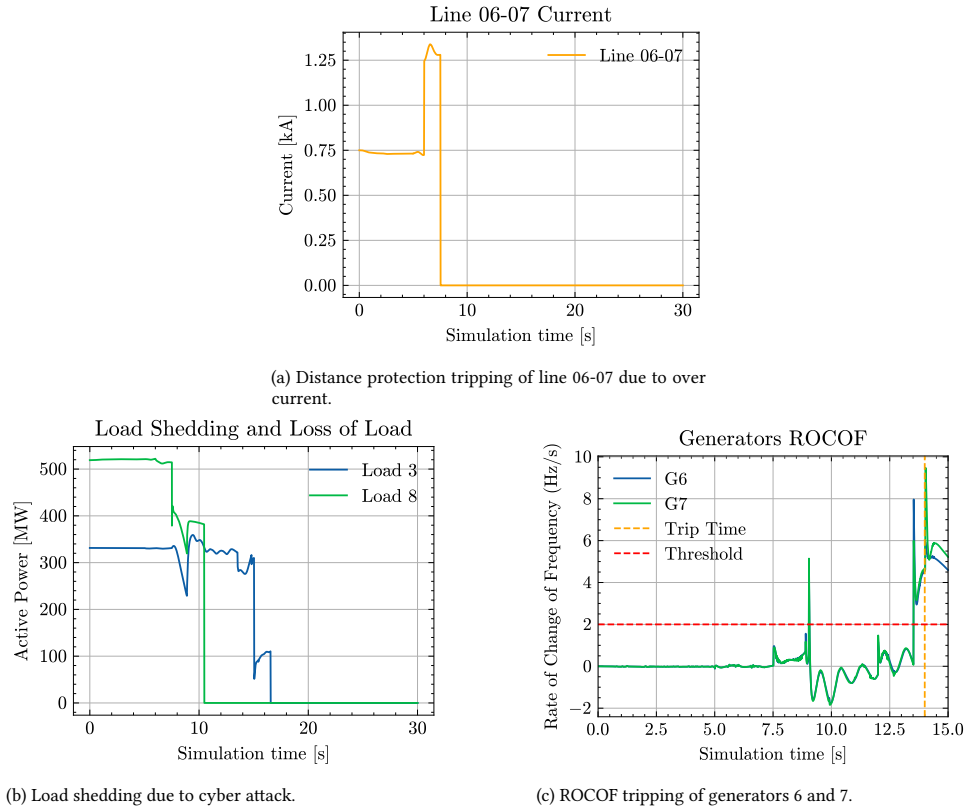


Figure 4.5: Power system dynamics and cascading failures caused by cyber attack on substation 14 and 21.

### Cyber Attack on Substation 9

In this scenario, only substation 9 is subjected to a cyber attack that results in malicious disconnection of all lines within the substation. As a result, the generator connected to the substation, G2 is islanded and tripped by ROCOF protection at 7.5s. Consequently, the system is destabilized due to the  $N - k$  contingencies and multiple transmission lines are disconnected leading to load shedding. Eventually, multiple generators are tripped by over frequency protection resulting in a partial blackout, as can be observed in Figure 4.6. The total loss of load is 3700 MW and the sequence of events is summarized in Table 4.3.

### Automatic Voltage Regulator Spoofing

In the presented attack scenario, a coordinated cyber attack leads to manipulation of generator AVR and opening of circuit breakers. The cyber attack is launched at 5s simulation time to maliciously alter the AVR set-point for generator G6, as visualized through Figure 4.8a. It is observed that the traffic is zero at some instants. This is due to variability

Table 4.2: Sequence of cascading failures due to cyber attack on substations 14 and 21.

| No. | Time          | Event                                                                                                                                                                                     |
|-----|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | 0s            | Start of simulation.                                                                                                                                                                      |
| 2.  | 5s to 7s      | Cyber attack on substation 14. Lines 05-06, 04-05, and 05-08 maliciously disconnected.                                                                                                    |
| 3.  | 7.5 to 9.0s   | Multiple lines tripped by distance protection, i.e., lines 06-07, 13-14. Also, distance relay 01-02 is tripped.                                                                           |
| 4.  | 9.5s          | Generators G2 and G3 trip due to ROCOF protection.                                                                                                                                        |
| 5.  | 10.4s         | Line 08-09 trips on distance protection. Area 1 is unsupplied.                                                                                                                            |
| 6.  | 11 to 12s     | Cyber attack on substation 21. Lines 16-24 and 23-24 maliciously disconnected.                                                                                                            |
| 7.  | 13.5s         | Distance relay trips line 21-22.                                                                                                                                                          |
| 8.  | 14s           | Generators G6 and G7 disconnect due to ROCOF.                                                                                                                                             |
| 9.  | 14.6 to 16.5s | Lines 02-03, 16-19, 17-27, 25-26, and 26-27 trip due to distance protection. G5 disconnects due to ROCOF. Load shedding (6.7% and 6.5%).                                                  |
| 10. | 17 to 18.2s   | Generators G8 and G9 disconnect due to ROCOF                                                                                                                                              |
| 11. | 30s           | End of simulation. Cyber attack results in islanding. Three islands remain with external grid, G4 and G10 supplying loads L20, L25 and L39. Total loss of load amounts to nearly 4000 MW. |

Table 4.3: Sequence of cascading failures due to cyber attack on substation 9.

| No. | Time           | Event                                                                                                         |
|-----|----------------|---------------------------------------------------------------------------------------------------------------|
| 1.  | 0s             | Start of simulation.                                                                                          |
| 2.  | 5s to 7s       | Cyber attack on substation 9. Lines 06-05, 06-07, and 06-11 disconnected.                                     |
| 3.  | 7.5s           | Generator G2 trips due to ROCOF protection.                                                                   |
| 4.  | 13.1s to 16.1s | Multiple lines trip due to distance protection, i.e., 04-14, 03-04, 16-17, 08-09, and 09-39.                  |
| 5.  | 18s to 21s     | Sustained under frequency activates load shedding of 5.9% on multiple loads.                                  |
| 6.  | 21.9s          | Generators G3, G4, G5, G6, and G7 trip due to over-frequency protection.                                      |
| 7.  | 30s            | End of simulation. Cyber attack results in partial blackout. Area 3 is islanded. Loss of load nearly 3700 MW. |

of latency and delays in distributed communication systems, leading to variations in the packet arrival time. The attack causes an abrupt increase in the terminal voltage of the generator by 10%. The cyber attack affects the voltage regulation and reactive power compensation factors. Subsequently, circuit breakers on the line 19-16, at substation 7 are also maliciously opened at 10s simulation time. As a result, the two generators in substation 7,

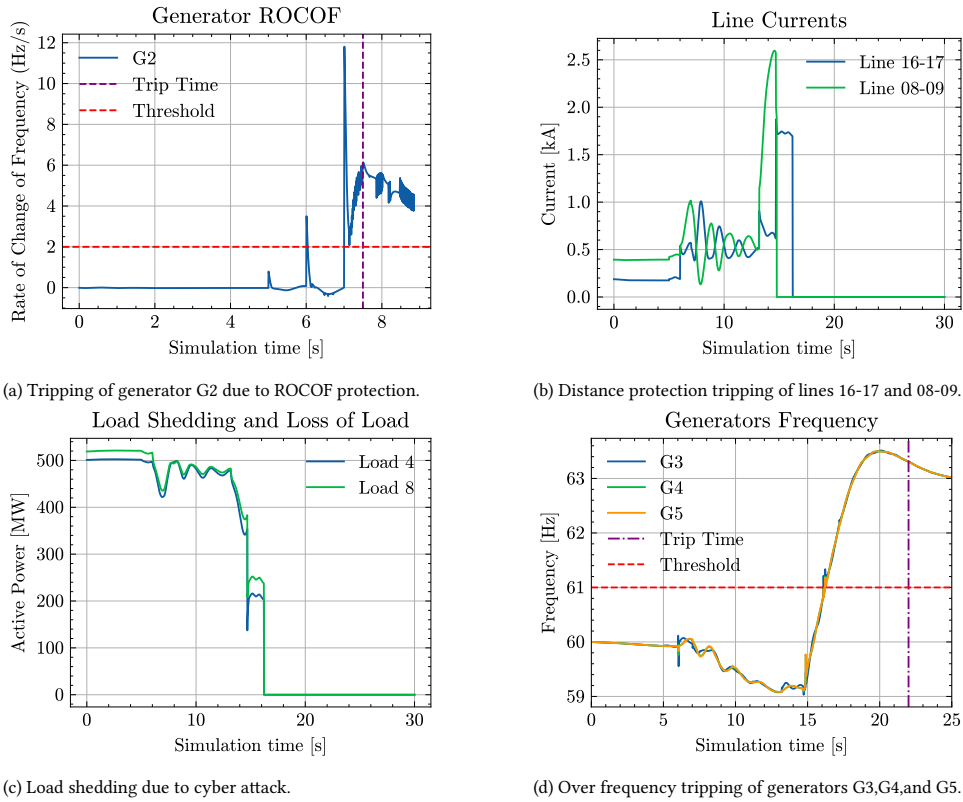


Figure 4.6: Power system dynamics and cascading failures caused by cyber attack on substation 9.

i.e., G4 and G5 are isolated from the rest of the system and disconnected by ROCOF protection. This can be visualized through Figure 4.8b, wherein the threshold of 2 Hz/s over 500 ms is crossed. Consequently, due to the sudden loss of generation, multiple transmission lines are overloaded and trip due to zone-3 distance protection. The sustained over-current and low voltage is misinterpreted as an uncleared zone-3 fault, resulting in an overreach of distance protection. This is depicted in Figure 4.8c as a plot of bus voltages and line currents highlighting sustained under voltage and over-current conditions.

Eventually, the generator targeted by the cyber attack, i.e., G6 is disconnected due to voltage instability around 13s, as predefined voltage limits (1.1 p.u) are exceeded. This is illustrated in Figure 4.8d. Therefore, the system is heavily stressed and the last remaining generator G7 in the vicinity of the attack location cannot cover all the loads and is isolated by ROCOF protection at 13.28s. This results in major system-wide frequency and voltage instabilities due to the loss of generation. Consequently, system frequency is severely affected due to the prolonged power mismatch, prompting emergency under frequency load shedding, as shown in Figure 4.8e. Following this, multiple lines are tripped by zone-3 distance protection overreach. Thus, the system reaches a point of no return at  $\approx 20$ s and the cyber attack results in a blackout with 5.2 GW load lost. The evolution of the cascade

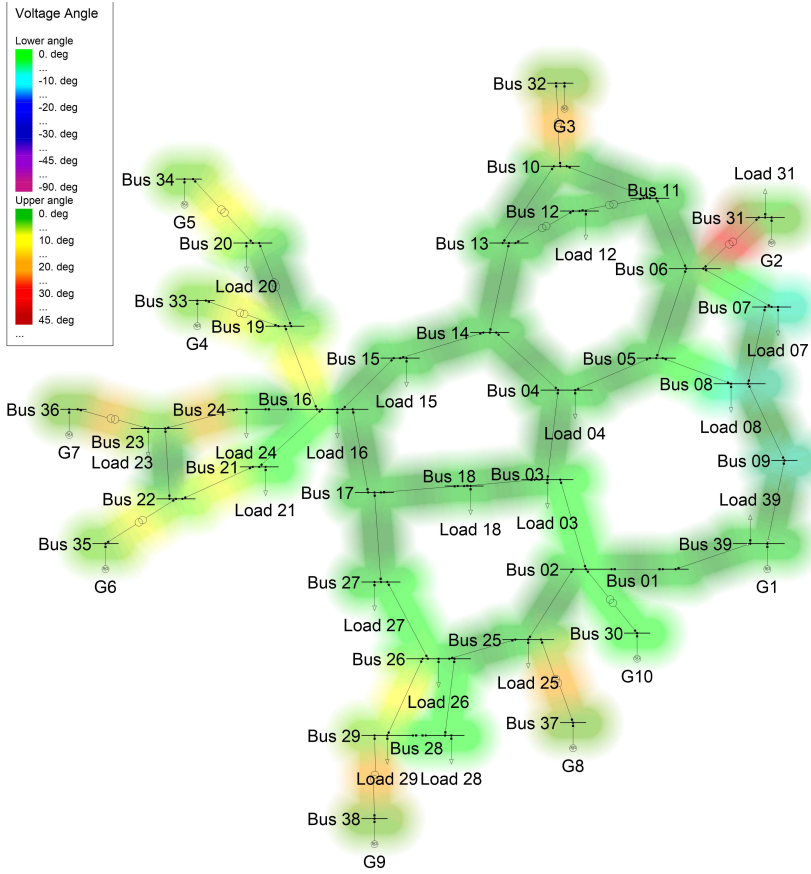
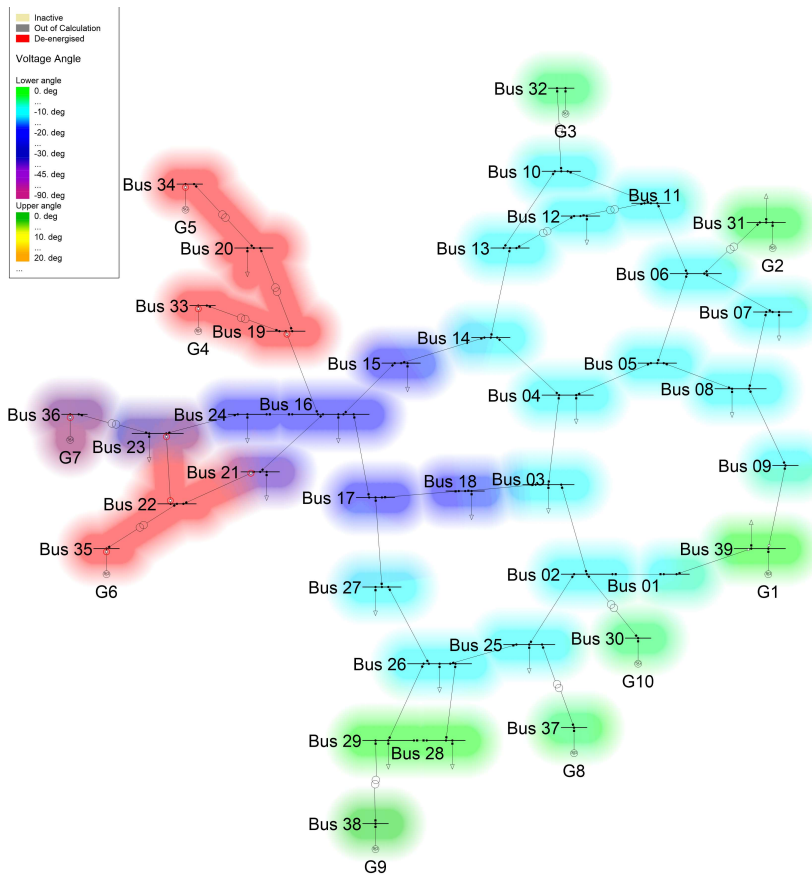
(a) Heatmap of voltage at  $t = 0s$ .

Figure 4.7: Propagation of cyber attack induced cascading failure on the IEEE 39-bus test system, visualized as heat maps of voltage angles. (Part 1) Top: 0s simulation time.



(b) Heatmap of voltage at  $t = 15\text{s}$ .

Figure 4.7: (Part 2) Middle: 15s simulation time.

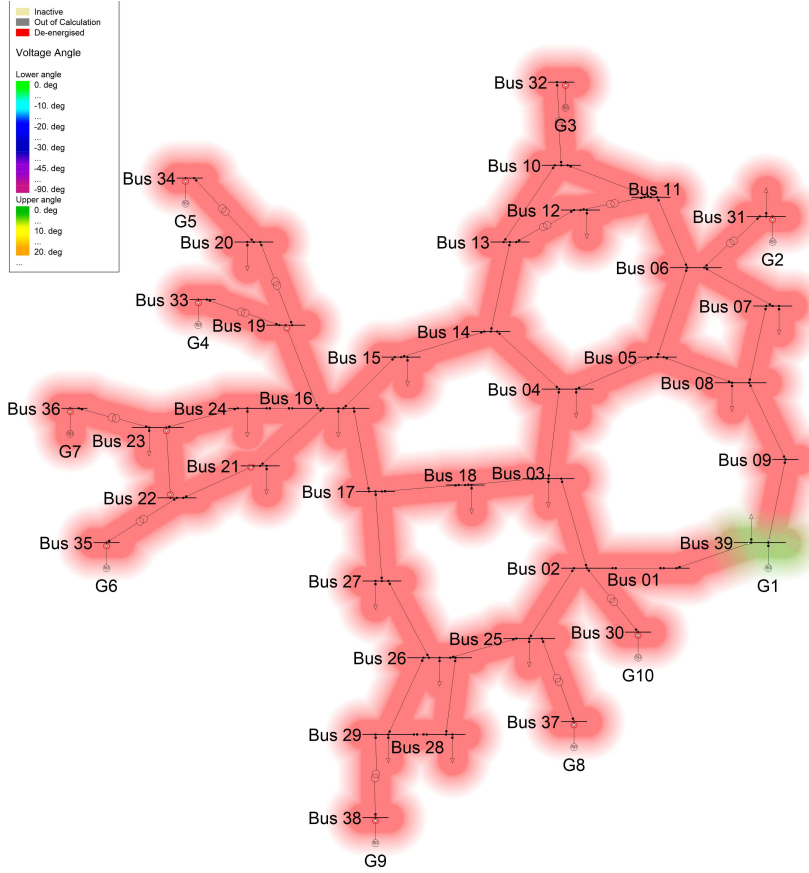
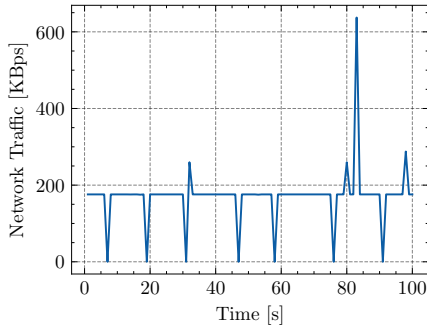
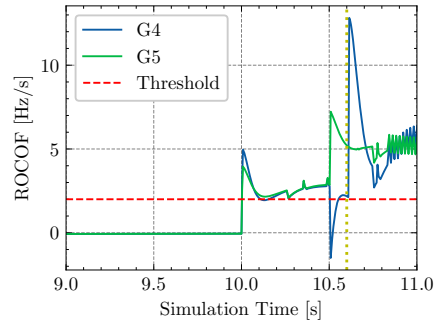
(c) Heatmap of voltage at  $t = 20s$ .

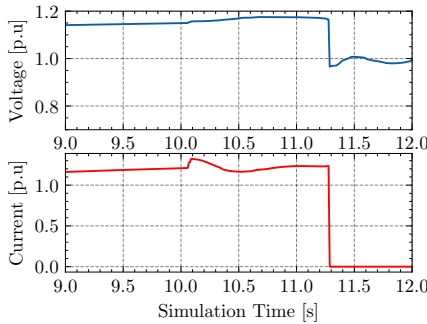
Figure 4.7: (Part 3) Bottom: 20s simulation time.



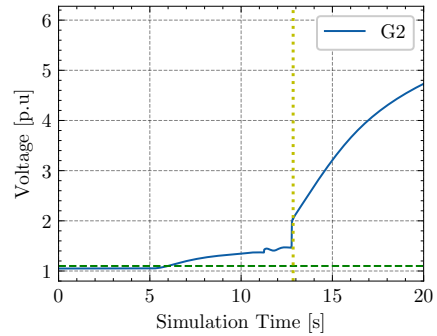
(a) Illustration of cyber attack via change in network traffic of substation 6 gateway.



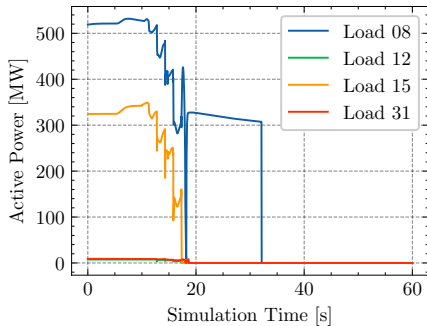
(b) ROCOF trip of generators G4 and G5. Protection setting limit is 2 Hz/s over 500 ms.



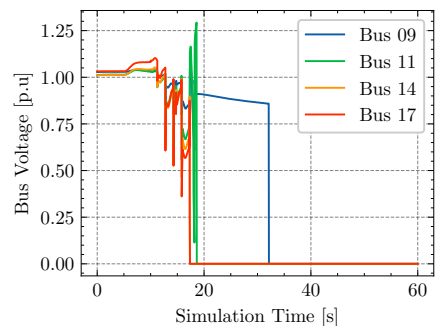
(c) Under voltage at bus 21 and overcurrent on line 21-22, highlighting trip of zone 3 distance protection.



(d) Over voltage trip of generator G2 at 12.8 s. Protection setting limit is 1.1 p.u. as shown by the green dashed line.



(e) Load shedding and loss of load due to cyber attack



(f) Voltage collapse caused by cyber attack.

Figure 4.8: Cascading failure dynamics due to spoofing cyber attack.

is better visualized through Figure 4.7 that illustrates variations in voltage angles over the course of the simulation. At the start of the simulation, most areas are healthy, i.e., with minimal voltage angle deviations (shown in green). Over the course of the cyber attack simulation, areas in red are de-energized, while the areas indicated by purple and blue suffer from power swings with significant variations in voltage angles, in excess of 30 to

40 degrees. The cyber attack results in a blackout in a matter of 20 s with 5.2 GW load being lost. The entire sequence of events is summarized in Table 4.4. As observed, the cyber attacks trigger multiple critical cyber-physical factors and influence the cascading failure mechanism. This results in a blackout, thereby confirming our hypothesis.

Table 4.4: Sequence of cascading failures due to AVR spoofing cyber attack.

| No. | Time       | Event                                                                                          |
|-----|------------|------------------------------------------------------------------------------------------------|
| 1.  | 0s         | Start of simulation.                                                                           |
| 2.  | 5s         | Spoofing cyber attack on substation 5. Generator G6 AVR set point increased by 10%             |
| 3.  | 10s        | Cyber attack at substation 7. Line 19-16 maliciously disconnected                              |
| 4.  | 10.5-10.6s | Generators G4 and G5 are islanded and disconnected by ROCOF protection.                        |
| 5.  | 11.2-12.7s | Lines 21-22, 22-23, and 23-24 trip due to distance protection.                                 |
| 6.  | 12.8s      | Generators G2 and G6 are disconnected by overvoltage protection.                               |
| 7.  | 13.27s     | Generator G7 is islanded and disconnected by ROCOF protection.                                 |
| 8.  | 14s-14.2s  | Under-frequency load shedding of 6.7% at all loads.                                            |
| 9.  | 14.28s     | Line 02-03 trips due to distance protection.                                                   |
| 10. | 14.3-17.3s | Load shedding                                                                                  |
| 11. | 17.31s     | Multiple lines trip due to distance protection, i.e., lines 04-05, 10-13, and 13-14.           |
| 12. | 17.52s     | Line 01-39 disconnects due to distance protection.                                             |
| 13. | 18.01s     | Generator G9 is tripped by ROCOF protection.                                                   |
| 14. | 20s        | End of simulation. Cyber attacks result in a blackout with loss of load amounting to ~5250 MW. |

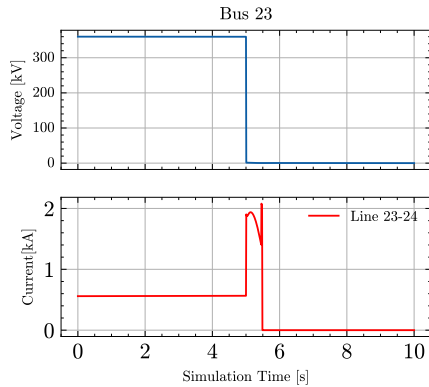
### Cyber-Physical Attack

This attack scenario exploits vulnerabilities in interlocking schemes within a digital substation, as previously explained. Furthermore, all protection functionality within the substation is inhibited due to a data modification attack. The malicious opening of a disconnect under loading, coupled with the lack of protection action results in a busbar fault on bus 23 at 5s simulation time. Subsequently, the non-timely clearance of the fault induces cascading failures throughout the system, resulting in a blackout. The sequence of events in the cascading failure is summarized in Table 2.3. As the protection equipment within the substation is inhibited due to the cyber attack, neighbouring lines are tripped by distance protection at 5.5 s simulation time. The loss of line 13-14 due to distance protection mis-operation, as previously explained, is depicted in Figure 4.9. As a result, the system is split into multiple islands with generator G6 being tripped by ROCOF protection at 6.2 s simulation time. The cascading loss of elements continues with the loss of other transmission lines. Subsequently, at around 6.8 s simulation time, multiple generators lose synchronism and are disconnected from the grid. This is visualized in Figure 4.9. The loss of multiple generators and lines destabilizes the power system with a lack of reactive power generation and extremely poor voltage profile. Finally, generators G2 and G3 trip due to sustained under voltage conditions of 0.8 p.u over 2 seconds at 8.7 s simulation time, resulting in a blackout. This is illustrated in Figure 4.9d.

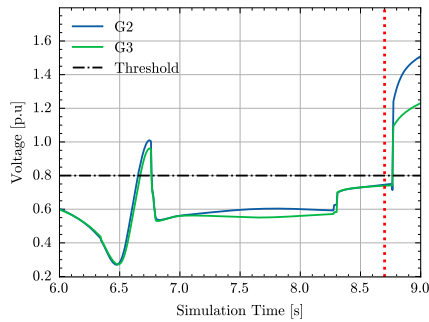
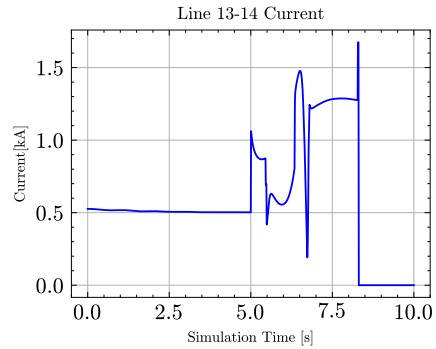
## 4.5.2 Point-of No-Return Identification

### Switching Attacks

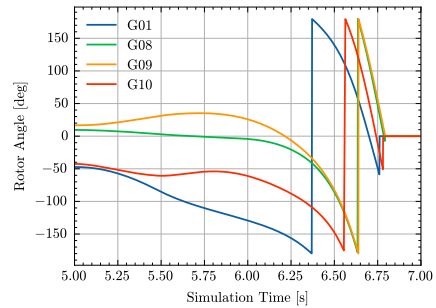
To verify the efficacy of the proposed method, two simulation case studies are compared. Scenario 2 is the opening of line 05-06 and Scenario 3 is the disconnection of all lines



(a) Busbar fault on bus 23.

(c) Under voltage trip of G2 and G3 at 8.7s simulation time. Protection setting is  $< 0.8p.u$  and  $t > 2s$ .

(b) Distance protection tripping of line 13-14 at 8.3s simulation time.



(d) Loss of synchronism of multiple generators.

Figure 4.9: Power system dynamics and cascading failures caused by cyber-physical attack.

Table 4.5: Sequence of cascading failures due to cyber-physical attack.

| No. | Time       | Event                                                                                                      |
|-----|------------|------------------------------------------------------------------------------------------------------------|
| 1.  | 5s         | Cyber attack causes busbar fault on bus 23.                                                                |
| 2.  | 5.5s       | Multiple lines in vicinity of attack location tripped by distance protection, i.e., lines 21-22 and 23-24. |
| 3.  | 6.1s       | Generator G6 is islanded and tripped by ROCOF protection.                                                  |
| 4.  | 6.1 – 6.3s | Multiple lines tripped by distance protection, i.e., lines 22-23 and 16-19. PNR is reached.                |
| 5.  | 6.6 – 6.7s | Lines 13-14 and 04-05 tripped by distance protection.                                                      |
| 6.  | 6.8s       | Multiple generators, i.e., G1, G8, and G9 lose synchronism.                                                |
| 7.  | 7.3s       | Generator G10 is islanded and tripped by ROCOF protection.                                                 |
| 8.  | 8.7s       | Generators G3 and G2 are disconnected by under voltage protection.                                         |
| 9.  | 10s        | End of simulation. Cyber attack results in loss of load ~6000 MW.                                          |

in substation 2. Both cases have initiating events at  $t=5s$  simulation time. Owing to the system topology, scenario 3 results in cascading failures, while the scenario 2 results in system disturbances. This is visualized through the voltage plot of bus 20 in Figure 4.10. For ease of explanation and analysis, sliding time windows are chosen as  $T_1 = [15, 20]$ ,  $T_2 = [20, 23]$ . Subsequently, the instantaneous damping is calculated to form the correlation matrix.

For scenario 2, in  $T_1$ , the system suffers significant oscillations, which are, however, well-damped, i.e.,  $\alpha(t) > 0$ . On the other hand, for scenario 3, as can be seen, the oscillations are undamped and rising, i.e.,  $\alpha(t) < 0$ . In time window  $T_2$ , however, the system reaches a new equilibrium point in scenario 2. This is visualized through Figure 4.11a which illustrates the correlation matrix  $R$  of damping values as a heat-map. As can be seen, most of the elements do not exhibit any correlation, shown in shades of blue. Furthermore, the difference in largest singular values between the successive time windows is infinitesimally small, i.e.,  $\Delta\sigma_1 \ll 0$ . Conversely, for scenario 3, during the propagation of cascade, the system moves from one instability point to another. This is indicated by an increase in positive correlations, as indicated by the heat-map in Figure 4.11b. More importantly, for scenario 3, the difference in largest singular values between time windows  $T_1$  and  $T_2$  is greater than zero, i.e., limit criterion (18) is violated. This is confirmed by a large positive shift of  $\approx 0.89$  in  $\Delta\sigma_1 \ll 0$  and can be visualized in Figure 4.12a (in red). Hence, it is concluded that the PNR is reached at ca 23s simulation time. Therefore, in scenario 3 from the initiating event, the PNR is reached in  $\approx 16$  seconds.

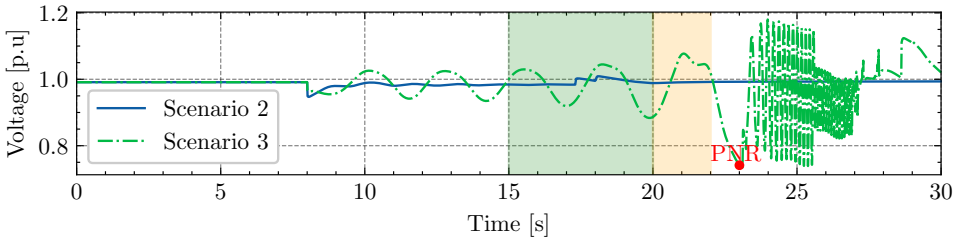


Figure 4.10: Comparison of voltages at bus 20 due to switching cyber attack.

To further analyze the active modes during these extended periods of instability, a detailed frequency analysis is carried out and is illustrated in Figure 4.12b. This corresponds to the time window  $T_2$  for bus 10. A similar result can be obtained for the other twelve PMU locations. Typical inter-area oscillations in power systems are observed to be in the range of 0.1 to 0.7 Hz. As can be observed from Fig. 7, closer to the PNR, the major oscillatory modes correspond to 1.2 and 1.5 Hz. Hence, these higher frequency oscillation modes correspond to the excitation brought about by cyber-physical events. These oscillations, if left unchecked, can lead to a system wide instabilities. Thus, such insights are useful when designing power system stabilizers or damping controllers.

### Spoofing Attack

To verify and validate the applicability and accuracy of the method, a spoofing and switching attack, i.e., Scenario 4, as described in Section III is simulated. In this attack scenario, the voltage reference set points for the AVR of generator G6 are maliciously spoofed by +10% at 5s simulation time. Simultaneously, two transmission lines, i.e., 16-19 and 16-24, are maliciously disconnected via a switching attack. These unexpected events result in the propagation of cascading failures throughout the system. Fig. 8 shows the plot of the voltage and time windows considered for analysis, using the proposed method. Similar to the analysis of the previous case, sliding time windows are chosen as  $T_1 = [5, 12]$ ,  $T_2 = [12, 17]$ .

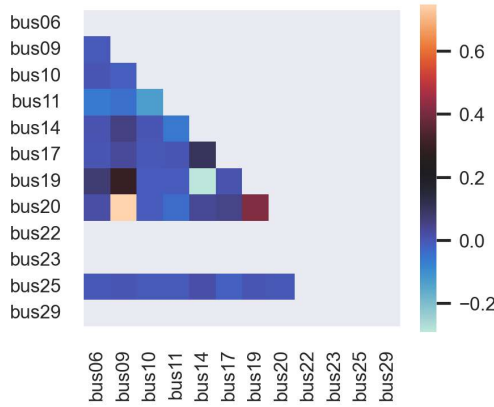
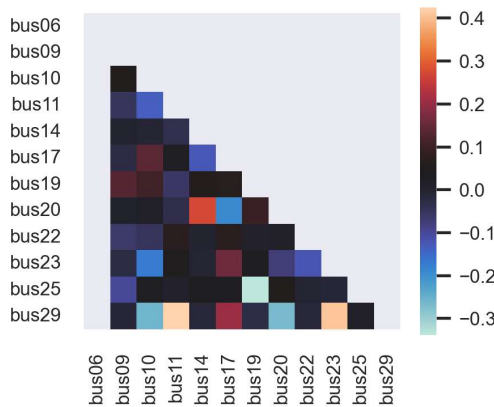
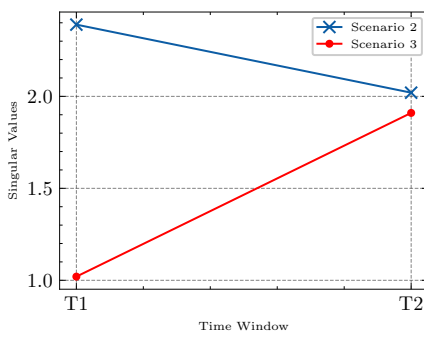
(a) Correlation matrix in time window  $T_1$ .(b) Correlation matrix in time window  $T_2$ .

Figure 4.11: Heat map comparison of correlation matrices.

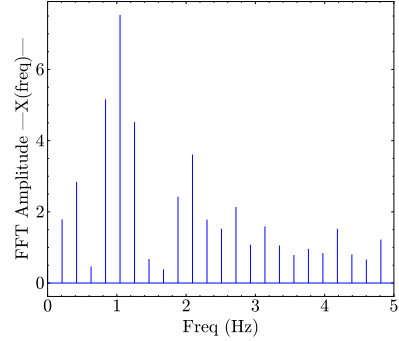
Subsequently, the instantaneous damping is calculated to form the correlation matrix. Due to the abrupt set point change and line disconnections, the system undergoes severe voltage stability issues. Crucially,  $\Delta\sigma_1 \approx 1$  in  $T_1$  and  $\Delta\sigma_1 \approx 1.28$  in  $T_2$ . Therefore,  $\Delta\sigma_1 \gg 1$  indicates that the point of no return lies in time window  $T_2$ . Eventually, the cyber attacks result in a blackout with 3000 MW load left unserved. The entire sequence of events of the cascading failure is summarised in Table xx.

### 4.5.3 Acceleration Mechanism

To study the acceleration of cascading failures, we analyze the Italy 2003 blackout. Figure 4.15a illustrates the observed cumulative loss of elements, based on the post incident report. As seen, until the point of no return, a linear behaviour is observed. Beyond this,



(a) Identification of point of no return through singular values.



(b) Frequency spectrum of bus 10 voltage in time window  $T_2$ .

Figure 4.12: Identification of point of no return.

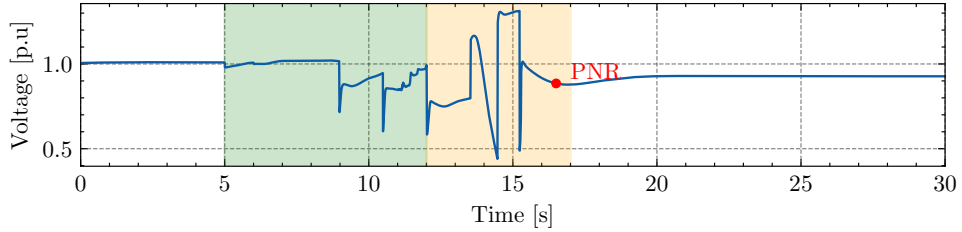


Figure 4.13: Voltage plot of bus 6. Time window  $T_1$  is from 5 to 12s, while  $T_2$  is from 12 to 17. The PNR is reached at  $\approx 16.5$ s.

Table 4.6: Sequence of events leading to cascading failures and blackout

| No. | Time        | Event                                                                                 |
|-----|-------------|---------------------------------------------------------------------------------------|
| 1.  | 5 s         | Spoofing cyber attack causes AVR voltage setpoint of generator G6 to increase by 10%  |
| 2.  | 5 – 6 s     | Lines 16-19 and 16-24 disconnected by switching attacks.                              |
| 3.  | 9 s         | Line 21-22 tripped by distance protection.                                            |
| 4.  | 9.5 s       | Generator G6 and G7 are islanded and tripped by ROCOF protection.                     |
| 5.  | 11 s        | Underfrequency load shedding by 7%.                                                   |
| 6.  | 12 – 13.5 s | Multiple lines tripped by distance protection, i.e., lines 26-27, 04-05, and 05-06    |
| 7.  | 14.3 s      | Generator G9 is islanded and tripped by ROCOF protection.                             |
| 8.  | 14.8 – 15 s | Generators G6 and G7 tripped by frequency protection. PNR is reached.                 |
| 9.  | 20 s        | End of simulation. Cyber attacks result in blackout with loss of load $\sim 3000$ MW. |

an exponential rise in loss of elements occurs. Hence, it is concluded that the point of no return was reached approximately in  $\approx 28$  minutes from the loss of the first element. Keeping this in mind, we simulate a scenario to mimic a similar sequence of events as illustrated in Figure 4.14.

In the considered scenario, routine maintenance causes line 05-06 to be put of service at 5s simulation time. Shortly thereafter, due to contact with vegetation, line 16-19 is also put of service at 10s simulation time. Consequently, the system is stressed, and other lines

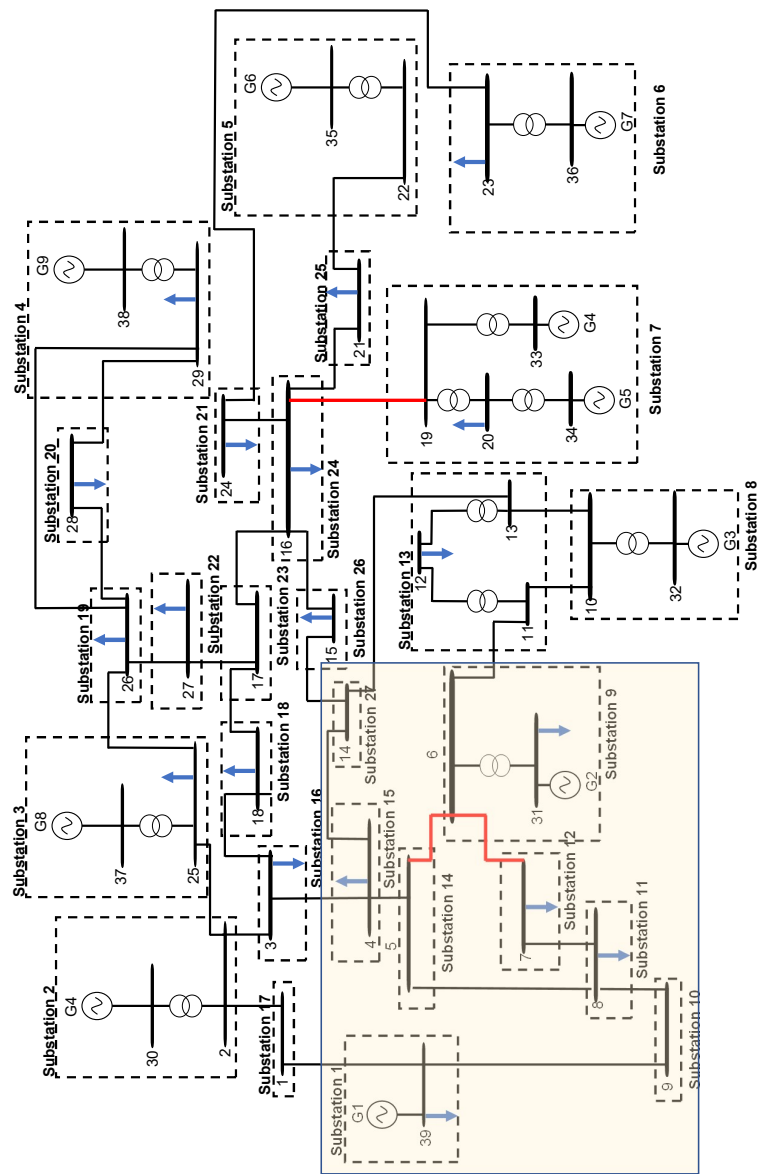
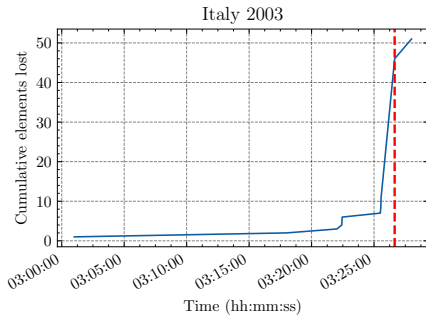


Figure 4.14: IEEE 39-bus single line diagram. The locations marked in red are disconnected, while the indicated area 1 is left unserved at the end of the simulation.

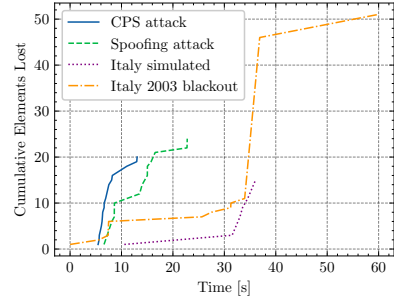
start to be overloaded. Eventually, line 06-07 comes in contact with vegetation and is immediately tripped at 30s simulation time. As a result, area 1 is blacked out. A comparison of the loss of elements in the between scenarios 1, 3, and 5 is carried out. The initiating events in all three scenarios occur at 5s simulation time and the cumulative loss of elements is depicted in Fig. 11. Furthermore, using the proposed method from this paper, the point of no return is calculated to be 10, 6.5, and 31s for cyber attack scenarios 3, 1 and 5, respectively. We use this information to define a rate of elements lost. The rate  $\gamma$  is defined as:

$$\gamma = \frac{\sum EL}{\Delta t} \quad (4.18)$$

where  $EL$  is the number of elements lost in a specific time period  $t$ . A comparison of the factor and final impact of the three cases is summarised in Table IV. As can be seen, attack scenario 1 is the quickest with a factor of almost 8.5, while scenarios 3 and 4 develop much slower. In case of the cyber attacks, multiple frequency modes  $> 1$  Hz are excited in a short time span, which when left unchecked lead to undamped system-wide oscillations. This can be attributed to the fact that cyber attacks can directly influence the occurrence of multiple events that are statistically improbable to occur together due to natural causes. Also, it can be seen that the ratio of PNR of scenario 5 to 1 is  $\approx 3$ . Thus, we empirically conclude that cyber attacks can induce a significant speed-up in the cascading failure mechanism, by at least a factor of 3x.



(a) Observed point of no return in the Italy 2003 blackout



(b) Acceleration of cascading failures due to cyber attacks.

Figure 4.15: (a) Point of no return in the Italy 2003 blackout, and (b) Acceleration of cascading failures due to cyber attacks.

Table 4.7: Comparison of cyber attack scenarios impact

| Scenario        | PNR (s) | $\gamma$ | Load Lost (MW) |
|-----------------|---------|----------|----------------|
| Spoofing        | 10      | 2.2      | 4000           |
| CPS             | 6.5     | 8.6      | 6000           |
| Italy simulated | 31      | 0.1      | 2500           |

## 4.6 Conclusions

The key findings of this chapter and related answers to research questions are summarized as follows. Based on these findings, the following chapter presents preventive controlled islanding to mitigate the impact of the cyber attack induced cascading failures before the point of no return is reached.

**RQ 1.2 and 1.3 How to prove semi-analytically that cyber attacks can cause and accelerate cascading failures in power systems?**

This chapter presented a data-driven analysis method to study how cyber attacks on power systems can induce accelerated large-scale cascading failures and a black-out. This involved time-frequency analysis of dynamic simulation data using a modified Hilbert-Huang transform. Additionally, using the proposed method and a synthetic case-study, it was shown how cyber attacks may accelerate the cascading failure mechanism by at least a factor of  $3\times$ . This is due to the excitation of multiple high frequency modes in a short time span. The analysis method was tested using time domain simulations conducted on a modified IEEE-39 bus test system, consisting of multiple, coordinated protection schemes. The proposed method can be used by utilities for cyber-physical system studies and assessment of cyber security and grid cyber resilience, which is currently of limited nature. Known limitations of the method include its a-priori nature and choice of the sliding time window.



## 5

## Preventive Controlled Islanding For Cyber Resilience

5

*Cyber-physical power systems are vulnerable to cyber attacks that may lead to cascading failures and power outages. A promising solution to tackle this emerging issue is the concept of preventive/proactive controlled islanding before the cyber event occurs based on early detection of cyber attacks. Hence, this letter proposes a novel physics-informed graph convolution network to perform preventive controlled islanding. By incorporating power system physics into the neural network loss function formulations, the resulting islands are made self-sufficient and voltage and frequency stable. Experimental simulations using the IEEE 39-bus test system with coordinated protection schemes show that the islands formed using the proposed method can contain the spread of cascading failures. This results in minimization of loss of load by up to 90% and 62% when single and multiple substations are compromised, respectively. Hence, this work paves the way towards cyber resilience of power systems.*

## 5.1 Motivation

Digitalization of the power grid, while offering advantages such as easier monitoring and control has brought cyber security into the spotlight. Multiple real-world cyber attack incidents targeting power systems have been reported globally. The most well-known are the attacks in Ukraine in 2015 and 2016, where cyber intrusions led to widespread power outages affecting hundreds of thousands of consumers [1]. More recently, in 2022, Ukraine was targeted again using never-seen-before attack tactics that exploited micro SCADA vulnerabilities. These incidents underscore the growing sophistication of cyber threats and the evolving tactics employed by attackers, which are no longer limited to conventional disruptions. Such attacks are increasingly targeted to induce and/or accelerate cascading failures, ultimately leading to catastrophic blackouts. The interconnected nature of power grids means that a successful attack on one part of the system can rapidly propagate, causing widespread outages and significant economic and social impact. Therefore, it is imperative to develop novel defense strategies that not only detect cyber intrusions [95], but also proactively mitigate or alleviate the impact of such attacks on the physical power network. Hence, the focus of this work is on preventive controlled islanding.

5

The two key challenges in islanding are – where and when to island? The former has been extensively studied in the literature [96, 97] using methods such as optimization [98] and graph theory [99]. For the latter, i.e., when to island, most existing methods work in response to an event/contingency such as a fault or disturbance. This type of islanding is therefore, reactive in nature. For example, in [97, 98], authors present optimization methods for islanding following a fault/short circuit, subject to various constraints such as generator coherency, island stability, etc. With the increased risk and threat of cyber attacks, however, the time to react following a cyber event is much shorter. This motivates the need for preventive or anticipatory islanding actions.

Bridging these gaps, this chapter introduces a novel preventive islanding solution using Physics-Informed Graph Convolutional Networks (PI-GCN) to contain cyber attack-induced cascading failures in power systems. The usage of physics-informed GCN is scientifically motivated by its ability to integrate power system physics into neural network loss functions, ensuring that the resulting islands are self-sufficient and stable in terms of voltage and frequency. By representing power systems as graphs, GCN can effectively capture both local and global dependencies, making them well-suited for modeling the spatial as well as temporal dynamics of power systems. Moreover, incorporating physical laws into the model increases its interpretability.

While preventive islanding has been briefly mentioned in the literature [100], our approach uniquely applies PI-GCN to dynamically assess and isolate vulnerable network areas in response to early-stage cyber attack detection. By embedding power system physics directly into the GCN's loss functions and constraints, the resulting islands are made dynamically stable in voltage and frequency. This is crucial given that cyber attacks can cause and accelerate cascading failures by a factor of  $3x - 4x$  [101]. The proposed model also addresses the complexities of advanced persistent threats, which may progress over days or months before any physical impact occurs. Therefore, by integrating early-stage intrusion detection systems [95] with our PI-GCN model enables proactive impact assessment and immediate preventive measures to contain and mitigate the possible cyber-induced cascading failures.

## 5.2 Physics-Informed Graph Convolution Network

### 5.2.1 Architecture

The islanding problem in power systems can be framed as a graph partitioning problem, which can be solved using deep learning techniques. In this chapter, a physics-informed GCN architecture is chosen to perform the islanding or clustering of nodes. A GCN is selected due to its inherent relational inductive bias, which emphasizes the aggregation of information from neighboring nodes. During training, the node embeddings are iteratively updated after each layer by incorporating features from adjacent nodes.

The architecture of the proposed GCN, illustrated in Fig. 1, consists of two GCN layers followed by a pooling layer. The pooling layer predicts the probability of each node belonging to a particular cluster, which is then used to derive the final cluster assignments and determine the necessary cutset. This method operates in an unsupervised manner, meaning it does not require labeled data for training the model. For the training, the power grid is represented as a graph,  $G = \{A, X, E\}$  and provided as input to the GCN, whereby  $A$  represents the associated adjacency matrix,  $X = \{(x_i)_k, i, k = 1, 2, 3 \dots n\}$  represents the nodal features, and  $E = \{e_j, j = 1, 2, 3 \dots m\}$  represents the edge features, respectively.

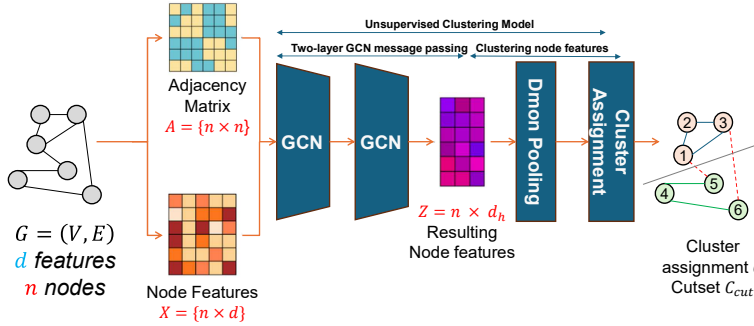


Figure 5.1: Architecture of the proposed PI-GCN model.

In this study, both spectral properties and power flow characteristics of the system are incorporated into the node features, yielding a total of seven features per node. The first three features capture the spectral properties of the graph: node degree and the two eigenvectors corresponding to the smallest non-zero eigenvalues of the normalized Laplacian matrix of the graph  $G$  [96]. The remaining four features—voltage magnitude, voltage angle, active power, and reactive power—are derived from an AC power flow calculation. Additionally, active power flows are employed as the edge weights in the graph. Therefore, each layer of the GCN can be represented as a function  $F$  with parameters  $\Omega$  that takes the node embeddings  $X$  and the edge weights  $E$  as inputs and outputs new node embeddings  $H$ . Hence, the convolutional process of the entire GCN can be summarized as follows:

$$H_k = F\{H_{k-1}, A, \Omega_{k-1}\} \quad (5.1)$$

where,  $k$  signifies the number of layers (depth of the GCN),  $H_k$  contains the updated node embeddings at the  $k^{th}$  layer, and  $\Omega_k$  denotes the parameters associated with that

layer. Furthermore, in this work, ReLu is used as the activation function  $F$  at each of the  $k$  layers, while Deep Modularity Network (Dmon) pooling introduced in [102] is used at the output layer.

### 5.2.2 Weight Adjustment for Isolation of Vulnerable Substations

The proposed preventive islanding method minimises the impact of cyber attacks by containing their potential physical impact. To achieve this, lines connected to the vulnerable substations as reported by the intrusion detection system are included in the splitting cut-set and removed during preventive islanding. Thereby, these substations are disconnected at the early stages of the cyber attack kill chain from the rest of the power system. Hence, during training, edge weights of attacked substations are set to zero. This influences the final pooling operation, favouring isolation of attacked nodes and ensuring that the GCN prioritizes system integrity and contains the spread of cascade.

To facilitate this requirement in the GCN model, the weights of the edges connected to the vulnerable substations are set to zero. This modification effectively prevents the vulnerable nodes from receiving information from their neighbours during the message passing phase of training. Consequently, the final pooling operation, based on the aggregated node features is influenced in a manner that favors isolation between the vulnerable nodes and their adjacent nodes. This approach ensures that the GCN prioritizes the integrity of the system's architecture and minimizes the propagation of potential adverse effects resulting from cyber attacks.

### 5.2.3 Loss Function and Constraints

The overall loss function to be updated at the end of each epoch is given as the sum of 3 individual loss terms, each of which is further detailed as below:

$$\mathcal{L}_N = (w_a \cdot \mathcal{L}_{cluster} + w_b \cdot \mathcal{L}_{conn} + w_c \cdot \mathcal{L}_{pbal}) \quad (5.2)$$

where,  $w_a, w_b, w_c$  represent the associate weight hyper-parameters to be fine-tuned during training. In the following,  $N$  represents the total number of training epochs, while  $n$  represents the number of clusters/islands to be formed.

- **Clustering loss:** this term is the loss function introduced in [102] as Deep Modularity Network which is based on modularity measure of clustering quality. Readers are encouraged to refer to [102] for a detailed formulation and explanation of the loss-term. Crucially, the Fiedler eigenvector, i.e., eigenvector corresponding to the second smallest non-zero eigenvalue of the normalized Laplacian matrix, captures the algebraic connectivity of the graph. Thereby, including it as node feature for training ensures connectedness of the formed islands.
- **Connectivity loss:** this term drives the model toward producing clusters that remain connected by penalizing disconnected nodes within clusters. For each of the predicted clusters, we identify disconnected nodes that do not belong to the largest connected component within the cluster. A binary mask array  $P$  is created where disconnected nodes are assigned a value of 1, and connected nodes are assigned 0. The connectivity loss is then computed using binary cross entropy (BCE) between

the predicted connectivity  $P$  and an ideal target of fully connected clusters, defined as:

$$\mathcal{L}_{\text{connectivity}} = \text{BCE}(P, \mathbf{0}) \quad (5.3)$$

where,  $P$  is a  $N \times 1$  array reflecting the disconnection status of the nodes.

- **Power-balance loss:** this loss term seeks to minimize the generation-load imbalance in each formed cluster/island and therefore embeds the physics into the training. It is given by:

$$\mathcal{L}_{pbal} = \sum_{i=1}^N \left( \sum_{i=1}^n G_i - \sum_{i=1}^n L_i \right)^2 \quad (5.4)$$

where  $G_i$  and  $L_i$  signify the generation and load demand, respectively. Furthermore, constraints are added to ensure adequate active and reactive power reserves in the islands, i.e.,  $\Delta P > 20\%$  and  $\Delta Q > 20\%$ . Additionally, each island contains at least one synchronous generator, to prevent a frequency collapse.

- **Island dynamic stability:** The proposed PI-GCN-based islanding approach ensures island stability through targeted loss functions and constraints that address both frequency and voltage stability. Each island is designed to include at least one synchronous generator, ensuring adequate inertia to maintain frequency stability under disturbances. Additionally, constraints on active power balance, i.e.,  $\Delta P$  further limits frequency deviations, preventing disconnection risks. It is assumed that voltage stability is supported by maintaining sufficient reactive power reserves using STATCOMs or shunt capacitors within each island, along with voltage constraints that prevent collapse. Together, these measures enable stable and resilient islands capable of containing the cascading failures, post-islanding.

### 5.2.4 Training and Clustering

The proposed PI-GCN method is implemented using PyTorch Geometric. pandapower is used to generate the training dataset. Additionally, DlgSILENT PowerFactory is used to validate the proposed islanding solution. The method is tested using the IEEE 39-bus test system with nominal loading conditions. GCN is initialized with the following characteristics and hyper-parameters, computed with Bayesian optimization [103].

- number of layers,  $k = 2$
- hidden layers = 128
- learning rate  $lr = 0.01$
- number of epochs  $N = 300$
- optimizer – Adam

## 5.3 Experimental Results

### 5.3.1 Case Studies

Two scenarios are considered as case studies, i.e., a single substation under attack and two substations under attack. We consider a spoofing attack that results in the malicious

disconnections of lines and generators. The specific attack vectors are described in [104]. The two scenarios are summarized as follows:

1. Single substation: we consider a cyber attack targeting substation 2, resulting in the disconnection of all circuits within the substation.
2. Two substations: we consider a cyber attack targeting substations 5 and 27 simultaneously, resulting in random disconnections of circuits within both substations.

The substation locations and disconnected components are highlighted in Fig. 5.2, while Table 5.1 summarizes both the case studies. For both cases, the base loading is 6097 MW. The validation of the islanding solutions of the GCN is performed through multiple time-domain simulations using a detailed dynamic power grid model equipped with protection relays. This model, introduced in [104] is capable of simulating cascading failures, allowing for a comprehensive evaluation of the resilience enhancement of the proposed islanding solutions.

Table 5.1: Summary of target locations and islanding cutsets

| Scenario            | Single substation                |                    | Two substations                         |                    |
|---------------------|----------------------------------|--------------------|-----------------------------------------|--------------------|
|                     | Component                        | Switching Time (s) | Component                               | Switching Time (s) |
| Targeted Components | Line 01-02                       | 15                 | G6                                      | 16.3               |
|                     | Line 02-25                       | 15.5               | Line 04-14                              | 17.8               |
|                     | G10                              | 16                 | Line 21-22                              | 18.8               |
|                     | Line 02-03                       | 16.5               | Line 22-23                              | 19                 |
|                     |                                  |                    | Line 14-15                              | 20.5               |
|                     |                                  |                    | Line 13-14                              | 20.6               |
| Islanding Cutset    | Lines 01-02, 02-03, 03-18, 14-15 | 1                  | Lines 01-39, 03-04, 14-15, 21-22, 22-23 | 1                  |

### 5.3.2 Dynamical Analysis of Preventive Islanding

#### Single substation

In this scenario, substation 2 is targeted by a malicious cyber attack resulting in disconnection of its lines between 15 – 17s simulation time. This results in a sudden  $N - 4$  contingency, causing system-wide instabilities. This can be observed from Fig. 5.3a, wherein in the absence of preventive islanding, large oscillations arise following the attack, destabilizing the system and resulting in tripping of more generators by protection relays, which in turn further propagates the cascade. As a result, there is in a major loss of load and a blackout.

In contrast, the application of preventive islanding at 1s significantly mitigates the impact. While the system initially experiences minor transients, it stabilizes shortly afterward. This can be observed by the plots in Figure 5.3b wherein the generator frequencies of two reference generators in the respective islands are shown. As can be seen, eventually the frequencies reach an equilibrium point at around 60s. More importantly, after the

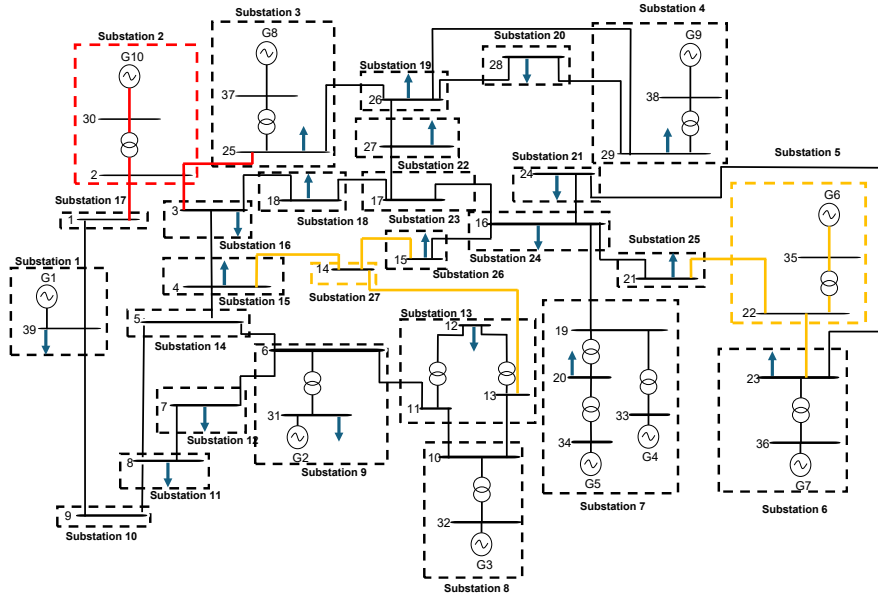
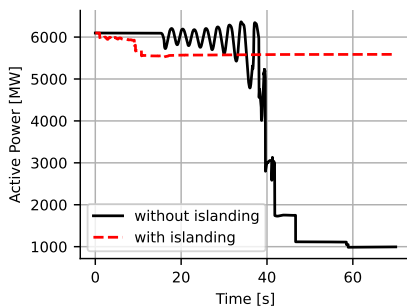
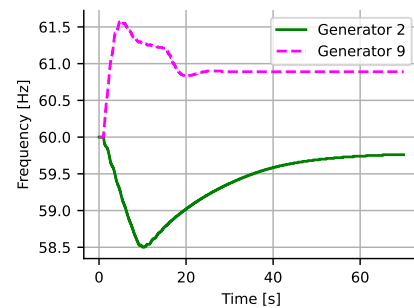


Figure 5.2: IEEE 39-bus single line diagram with substations and cyber attack locations. Single substation attack is shown in red, while multiple substation attack is shown in orange.

occurrence of the cyber attack, the effect is nearly nullified due to the preventive isolation of two critical substation lines prior to the attack. The islanding action limits the cyber attack impact to minimal loss of load of 509 MW, in comparison to the situation without islanding, where nearly 5000 MW is lost. Figure 5.3a clearly highlights the benefit of the preventive islanding, leading to almost 90% savings of load.



(a) Comparison of total loss of load with and without islanding for single substation attack scenario.



(b) Frequencies of reference generators in respective islands for single substation attack scenario.

Figure 5.3: Comparison of total loss of load and frequencies for single substation attack scenario.

## Two substations

In this scenario, substations 5 and 27 are targeted by malicious cyber attacks that randomly switch off their connected lines between 16 – 21s simulation time, as depicted in Table 5.1. This sudden disconnection of components, instigates major cascading failures to spread throughout the system. In the case of no remedial and islanding actions, the system suffers a voltage collapse as depicted in Figure 5.4c and suffers a blackout with a total loss of load  $\approx 5617$  MW as seen in Fig. 5.4a. In contrast, when the preventive islanding is applied, the cascade propagation is halted and the system does not completely collapse, resulting in 1823 MW of load being lost. Furthermore, the resulting islands are dynamically stable as evidenced by their respective reference generator frequencies in Fig. 5.4b. Thus, due to the preventive islanding, saving in the loss of load of up to 62% is achieved. Additionally, Figure 5.5 depicts the single line diagram of the cutsets and formed islands, post the preventive islanding action.

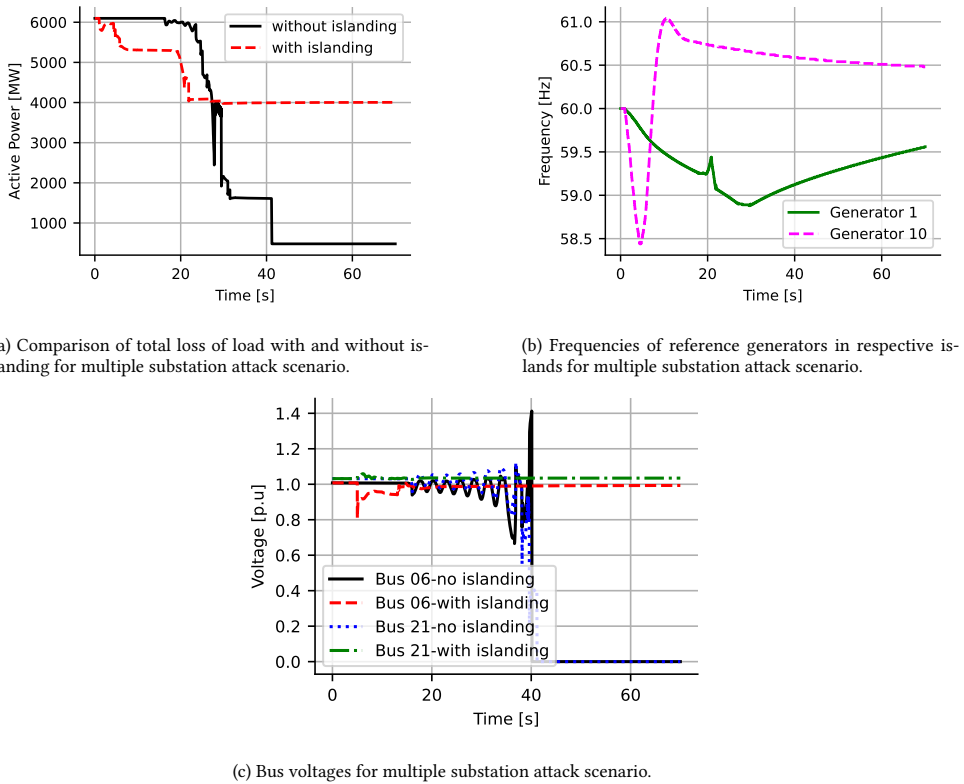


Figure 5.4: Comparison of power system dynamics with and without preventive islanding for multiple substation attack scenario.

## Comparison

A comparison between the two case studies is provided in Table 5.2. As can be inferred, in both cases, the application of preventive islanding results in significant improvement

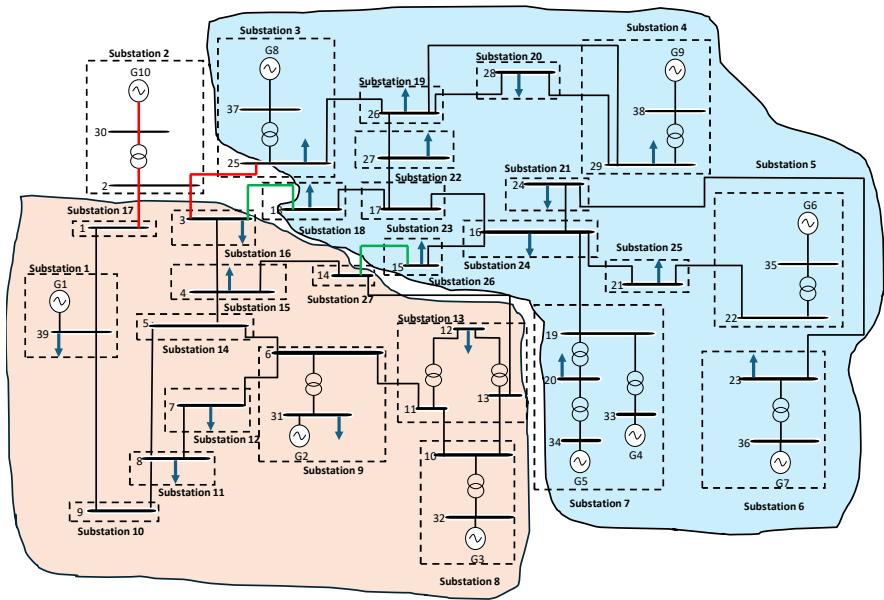


Figure 5.5: Single line diagram to visualize cutsets and islands. The lines shown in green are disconnected as part of the preventive islanding action.

regarding loss of load by up to 90% and 62%, respectively. Furthermore, even in the case of a false alarm, where a cyber attack is either successfully prevented or does not occur, the percentage of load lost is minimal, i.e., < 15%, which is acceptable compared to the risk if the attack does occur. This proves the effectiveness of the proposed preventive islanding approach.

Table 5.2: Comparison of cascading outage impact with and without islanding

| Metric                      | Without islanding | With islanding | False alarm islanding |
|-----------------------------|-------------------|----------------|-----------------------|
| Single substation attack    |                   |                |                       |
| Loss of load (MW)           | 5102.7            | <b>509.6</b>   | 504                   |
| Percentage Loss of load (%) | 83.7              | <b>8.4</b>     | 8.2                   |
| Number of Lines lost        | 32                | <b>5</b>       | 4                     |
| Two substations attack      |                   |                |                       |
| Loss of load (MW)           | 5616.6            | <b>2091.9</b>  | 889                   |
| Percentage Loss of load (%) | 92.1              | <b>34.3</b>    | 14.6                  |
| Number of Lines lost        | 34                | <b>15</b>      | 5                     |

## 5.4 Conclusions

The key findings of this chapter and related answers to research questions are summarized as follows.

**RQ 2.2** How to mitigate the impact of cyber attacks using proactive approaches to contain the spread of cascading failures in power systems?

This chapter presented preventive controlled islanding which is a proactive solution to mitigate the risks of cyber attacks, before they escalate or even occur. To this end, this chapter introduced a physics-informed graph convolution network for preventive islanding. It is seen that integrating power system physics into the loss functions ensures self-sufficiency and transient stability of the formed islands. Simulation results on the IEEE 39-bus system demonstrate the effectiveness of the proposed approach, showing up to a 90% and 62% reduction in loss of load when single and multiple substations are targeted by cyber attacks, respectively. This illustrates the effectiveness of preventive islanding in containing the spread of the cascading failures.

# 6

## Conclusions and Discussion

This chapter summarizes the key outcomes of this thesis, revisits the original research questions and provides answers to them. Furthermore, the major implications of this thesis and outlook for future work is also discussed.

### 6.1 Answers to Research Questions

This thesis was centered around five key research questions, posed in Chapter 1. In this section, we revisit and answer each of the research questions, alongside the associated scientific contributions and implications. The research questions and associated chapters are summarized below.

*RQ 1.1 How to show qualitatively and quantitatively that cyber attacks can cause cascading failures in power systems? (Chapter 2)*

*RQ 1.2 How to prove semi-analytically that cyber attacks can cause cascading failures? (Chapter 4)*

*RQ 1.3 How to prove semi-analytically that cyber attacks can accelerate cascading failures? (Chapter 4)*

*RQ 2.1 How to secure GOOSE messages to mitigate cyber attacks on digital substations? (Chapter 3)*

*RQ 2.2 How to mitigate the impact of cyber attacks using proactive approaches to contain the spread of cascading failures in power systems? (Chapter 5)*

**RQ 1 Can cyber attacks cause and accelerate cascading failures?**

**RQ 1.1 How to show qualitatively and quantitatively that cyber attacks can cause cascading failures in power systems?**

Chapter 2 delves into how cyber attacks can lead to cascading failures in power systems, addressing both qualitative and quantitative aspects. In the qualitative analysis, the

study begins with a systematic survey of major historical blackouts caused by physical disturbances. This survey provides a foundational understanding of the mechanisms behind cascading failures in power systems. By examining these historical events, the research identifies critical cyber-physical factors that can trigger and influence cascading failures. Building on this, the study qualitatively hypothesizes how cyber attacks on power grids can lead to cascading failures and blackouts by exploiting these critical factors.

To quantitatively demonstrate the impact of cyber attacks, numerical simulations and HIL-based experiments are conducted in Chapter 3 and Chapter 4. A modified version of the IEEE-39 bus test system is developed, incorporating multiple protection schemes to simulate cascading failures. This system is connected to an OT network emulator to perform cyber-physical co-simulations, assessing the impact of cyber attacks on power system dynamics. The effects of cyber attacks and their role in causing cascading failures are experimentally verified using a dedicated HIL setup, which closely mimics real-world conditions in a digital substation.

#### Key Findings

Our findings from Chapter 2 indicate a fundamental link between the power system cascading failure mechanism and cyber security. It is seen that critical cyber-physical factors that enable and influence the cascading failure mechanism can be influenced by cyber attacks. This is in addition to physical disturbances that are well-understood. Thus, the qualitative analysis establishes a clear and direct link between cyber attacks and their influence on the cascading failure mechanism. The implications of these findings are significant for both, utilities and policymakers. For utilities, it underscores the need for proactive investment in cyber security infrastructure and the development of robust incident response plans. Policymakers, on the other hand, must consider the broader implications of cyber threats on critical infrastructure and develop regulations that promote both cyber security and resilience. Hence, such an analysis paves the way toward cyber resilient power systems.

In conclusion, this research provides a comprehensive analysis of the link between cyber security and cascading failures in power systems. By reviewing historical blackouts and identifying critical cyber-physical factors, the study qualitatively establishes how cyber attacks can initiate cascading failures. The quantitative analysis, supported by simulations and experiments, further validates this hypothesis, highlighting the direct influence of cyber attacks on the cascading failure mechanism. The findings underscore the importance of robust cyber security measures in securing cyber-physical power systems from potential blackouts.

#### **RQs 1.2 and 1.3 How to prove semi-analytically that cyber attacks can cause and accelerate cascading failures in power systems?**

To answer these research questions, Chapter 4 introduces a data-driven analysis method to investigate how cyber attacks can induce and accelerate large-scale cascading failures in power systems. This method employs a modified Hilbert-Huang transform for time-frequency analysis of dynamic simulation data. By applying this approach, the chapter

demonstrates that cyber attacks can accelerate the cascading failure mechanism by at least a factor of three. This acceleration is attributed to the excitation of multiple high-frequency modes within a short time span, highlighting the potential for acceleration of the cascading failure mechanism. The proposed method was validated using time-domain simulations on a modified IEEE-39 bus test system, which includes multiple coordinated protection schemes. This setup allowed for a comprehensive assessment of how cyber attacks can impact power system dynamics, providing valuable insights into the vulnerabilities of modern power grids.

The research outcomes and answers to these questions offer several new insights and implications for the domain of power system cyber security. The research highlights the importance and impact of considering the temporal nature of power system dynamics caused by cyber attacks during the fast phase of cascading failure. Furthermore, by comparing cascading failures caused by physical disturbances against cyber attacks, demonstrates that cyber attacks can accelerate cascading failures. Hence, these crucial research findings highlight the need for real-time monitoring and rapid response mechanisms to mitigate the impact potential cyber disruptions. This insight is crucial for utilities seeking to enhance their cyber-physical system resilience.

#### Key Findings

Experimental results from Chapter 4 provides evidence that cyber attacks not only trigger cascading failures in power systems but also significantly accelerate their progression. Our key finding reveals that cyber attacks can speed up the cascading failure mechanism by at least a factor of three compared to historical blackouts caused by physical disturbances. This acceleration highlights the urgent need to develop solutions to address cyber security vulnerabilities in power systems, given their critical nature. These findings can aid in shifting the focus from traditional physical contingency analysis to a more holistic cyber-physical approach. This shift is essential for developing robust strategies that can mitigate the risks posed by cyber attacks and enhance the overall resilience of power systems to both physical and cyber disruptions. Therefore, by integrating cyber security considerations into their operational planning and system operations, utilities can better prepare for and respond to the evolving cyber threat landscape.

Moreover, the proposed method provides a practical tool for utilities to evaluate the cybersecurity posture of their power systems. By identifying the excitation of high-frequency modes as a key factor in accelerating cascading failures, the research paves the way for more targeted cybersecurity measures. This includes the development of protection schemes that can detect and respond to such anomalies in real-time. Overall, the research serves as a significant contribution to the field, offering a semi-analytical approach to understand the impact of cyber attacks on power systems.

**RQ 2** How to minimize and contain the impact of cascading failures caused by cyber attacks?

**RQ 2.1 How to secure GOOSE messages to mitigate cyber attacks on digital substations?**

To mitigate cyber threats within digital substations, the IEC 62351-6 standard introduces a framework for enhancing the security of GOOSE messages. This framework is designed to address the vulnerabilities inherent in digital communication protocols while maintaining the stringent real-time performance requirements of less than 4 milliseconds. The standard recommends integrating an additional field to the GOOSE data payloads to accommodate security-relevant information. This additional field is based on cryptographic hash algorithms, such as SHA-256, to generate a unique HMAC for every outgoing GOOSE messages. Thereby, spoofing and replay attacks are successfully thwarted.

Empirical results from Chapter 3 demonstrate that the implementation of HMAC can effectively mitigate the threats of spoofing and replay attacks targeting IEC 61850 GOOSE messages. These attacks, which involve the injection of fraudulent messages or the replay of legitimate ones, can lead to unwanted equipment disconnections and even cascading outages. Our proof-of-concept implementation shows that legacy GOOSE communications can be secured without significant changes to substation communication network architecture/topology. Most vendors do not yet support this standard, thereby bringing into focus the need for concerted efforts in development, standardization, and industry-wide collaboration to enhance the cyber security digital substations. Furthermore, the successful deployment of HMAC necessitates a robust key management infrastructure within the digital substation. This infrastructure must be maintained and regularly updated by substation operators to ensure the effectiveness of security measures. Hence, highlights a critical gap in the current cyber security posture of many digital substations that requires both technical and policy related overhauls.

**Key Findings**

Results from Chapter 3 prove that Hash-based Message Authentication Code can be implemented in digital substations to secure legacy GOOSE communications, adherent to the latency requirements of  $< 4ms$  as specified in IEC 62351-6. Hence, this proof-of-concept implementation demonstrates the applicability of proactive cyber security measures to safeguard digital substation communications.

In conclusion, Chapter 3 shows that IEC 62351-6 can be successfully implemented and it provides a cryptographically sound framework for securing GOOSE messages. Nevertheless, its full potential can only be realized through comprehensive key management infrastructures and wider industry support.

**RQ 2.2 How to mitigate the impact of cyber attacks using proactive approaches to contain the spread of cascading failures in power systems?**

The research findings from Chapter 5 highlight the effectiveness of an artificial intelligence-based proactive controlled islanding approach in proactively mitigating the impact of cyber attacks on power systems. This strategy demonstrates the efficacy of proactive islanding (pre-event), in comparison to reactive islanding (post-event), by minimizing load shed and ensuring the stability of the formed islands. The application of a physics-informed graph convolution network for the islanding process ensures that each island operates independently and remains voltage and frequency stable. This stability is crucial for maintaining operational continuity and preventing further disruptions within the isolated sections of the grid. Simulation results on the IEEE 39-bus system provide proof of the approach's effectiveness. The strategy achieves up to a 90% reduction in loss of load when a single substation is targeted and a 62% reduction when multiple substations are compromised. These significant reductions prove the method's efficacy to contain cascading failures and maintain grid stability, even under complex cyber attack scenarios.

#### Key Findings

Results from Chapter 5 illustrate the effectiveness of an artificial intelligence-based proactive controlled islanding approach, before any cyber event takes place. Results show the effectiveness of this approach in minimizing load shed, while ensuring the frequency and voltage stability of the formed islands. Such an approach is analogous to quarantining multiple neighborhoods in a city/town as a proactive measure, in response to an upcoming epidemic that has not yet occurred. Thereby, the spread of an infection (cascading outages) can be successfully contained.

In summary, by adopting such a proactive approach, utilities can significantly enhance the resilience of their power systems against cyber threats. The findings also underscore the applicability of advanced machine learning techniques based on physical principles to develop more effective and adaptive cyber security strategies. This innovative approach offers a promising avenue for safeguarding power systems against emergent cyber threats. Furthermore, this approach highlights the need for proactive measures and collaborative efforts between the OT and operational domains to establish robust cyber security measures.

## 6.2 Recommendations and Future Work

Based on the research outcomes of this thesis, following are the recommendations for future work:

- **Performance evaluation of HMAC:** Chapter 3 describes the successful implementation of a HMAC proof-of-concept to secure GOOSE communications. Nevertheless, further detailed research into the performance of the HMAC can be carried out. For example, a statistical analysis of the latency under different operating conditions such as faults, blocking, etc. Furthermore, additional investigations into usage of a real-time kernel or different hardware platforms, such as microcontrollers or FPGAs [105] may be carried out. Such research however, is interdisciplinary and challenging, as it requires good understanding of both power systems and computer engineering.

- **Intrusion detection and prevention systems with active countermeasures:** Our findings from Chapter 4 illustrate the urgency and threat of cyber attacks on power systems. With the increased risk and limited time to react (given the acceleration of cascading failures by  $3\times$ ), following cyber threats, advanced intrusion detection systems must be urgently developed. Such systems must be capable of early-stage cyber attack detection and serve as a “first warning.” Additionally, intrusion prevention capabilities may also be developed to restrict and contain potential cyber attacks only within the cyber space, without spilling over to the physical power grid. Therefore, active countermeasures must be taken at the security operations centre within the cyber space, in the early stages of the kill chain to prevent unavoidable impact on the physical power grid. This can include techniques such as network segmentation of the OT network or WAN communications, in response to a positive intrusion detection with high confidence. Furthermore, as proposed within this work, depending on the targeted regions/areas, worst-case impact analyses can be carried out to predict possible adverse consequences or cascading sequences. As a result, proactive situational preparedness in the face of an active cyber threat can be achieved. Such an approach is also now mandated by the European network code on cybersecurity in the face of ever increasing risks due to cyber threats. The code mandates that high and critical impact entities, such as power grids must establish cyber attack management procedures, including effective processes to identify, classify, and respond to cyber attacks.
- **Adaptive dynamical analysis and point of no return identification:** Some of the known limitations of the method used within Chapter 4 include its a-priori nature, i.e., known beforehand and choice of the sliding time window. Future work can focus on real-time or near real-time PNR prediction to overcome these limitations. This could be achieved by analysing the waveforms and dynamically adjusting the time windows when events are triggered. Furthermore, such work can integrate with advanced intrusion detection systems to form a comprehensive cyber-physical resilience framework.
- **Self-healing:** The concept and results of preventive controlled islanding was described in Chapter 5. Based on the findings from the chapter, future work can examine the impact of the disconnection cutset sequence on transient stability. Based on this, the optimal order in which lines should be disconnected to minimize disruptions can be identified. This may be achieved by performing a combinatorial analysis for a particular preventive islanding use-case and comparing the impact of the various disconnection sequences. It may well be possible, owing to specific grid topologies, opening particular lines first may result in transient instabilities within the islands. Furthermore, usage of dispatchable resources or generation can be explored to maintain the transient stability within the individual islands. Resynchronization techniques of the formed islands with the main grid also need to be further investigated. Additionally, post-islanding control strategies may be integrated to establish a comprehensive framework for automated power system self-healing. Such strategies could include special protection systems to maintain system equilibrium and operational integrity post islanding.

The societal implications of this research are critical. Power grids are the backbone of modern societies, supporting essential services such as healthcare, transportation, and communications. This research contributed to the broader goal of ensuring a cyber-resilient power system, which is crucial for societal well-being and economic stability. In conclusion, this thesis highlights the urgency and importance of addressing the risks posed by contemporary cyber threats to power systems. Furthermore, it emphasizes the need for proactive measures to safeguard critical infrastructures such as power grids.



## Bibliography

- [1] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *Proc Annual Conf for Protective Relay Engineers (CPRE)*, pages 1–8, College Station, TX, Apr 2017.
- [2] R.M. Lee, M.J. Assante, and T. Conway. Analysis of the Cyber Attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC) Tech Report*, pages 1–26, Mar 2016.
- [3] Chen Ching Liu, Alexandru Stefanov, Junho Hong, and Patrick Panciatici. Intruders in the grid. *IEEE Power and Energy Magazine*, 10(1):58–66, Jan–Feb 2012.
- [4] Chen Peng, Hongtao Sun, Mingjin Yang, and Yu Long Wang. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49:1554–1569, 8 2019.
- [5] Ian Dobson. Where is the edge for cascading failure?: challenges and opportunities for quantifying blackout risk. In *2007 IEEE Power Engineering Society General Meeting*, pages 1–8, 2007.
- [6] Shengwei Mei, Fei He, Xuemin Zhang, Shengyu Wu, and Gang Wang. An improved opa model and blackout risk assessment. *IEEE Transactions on Power Systems*, 24(2):814–823, 2009.
- [7] Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464:1025–1028, 2010.
- [8] Margaret J. Eppstein and Paul D. H. Hines. A “random chemistry” algorithm for identifying collections of multiple contingencies that initiate cascading failure. *IEEE Transactions on Power Systems*, 27(3):1698–1705, 2012.
- [9] M. Vaiman, P. Hines, J. Jiang, S. Norris, M. Papic, A. Pitto, Y. Wang, and G. Zweigle. Mitigation and prevention of cascading outages: Methodologies and practical applications. In *2013 IEEE Power & Energy Society General Meeting*, pages 1–5, 2013.
- [10] Rui Yao, Shaowei Huang, Kai Sun, Feng Liu, Xuemin Zhang, and Shengwei Mei. A multi-timescale quasi-dynamic model for simulation of cascading outages. *IEEE Transactions on Power Systems*, 31:3189–3201, 7 2016.
- [11] Jiajia Song, Eduardo Cotilla-Sanchez, Goodarz Ghanavati, and Paul D. H. Hines. Dynamic modeling of cascading failure in power systems. *IEEE Transactions on Power Systems*, 31(3):2085–2095, 2016.

- [12] Matthias Noebels, Ian Dobson, and Mathaios Panteli. Observed acceleration of cascading outages. *IEEE Transactions on Power Systems*, 36:3821–3824, 7 2021.
- [13] Matthias Noebels, Robin Preece, and Mathaios Panteli. Ac cascading failure model for resilience analysis in power networks. *IEEE Systems Journal*, 16:374–385, 3 2022.
- [14] G Ericsson. Cyber Security and Power System Communication. *IEEE Trans Power Delivery*, 25(3):1501–1507, Jul 2010.
- [15] Bo Chen, Karen L. Butler-Purpy, Sruti Nuthalapati, and Deepa Kundur. Network delay caused by cyber attacks on svc and its impact on transient stability of smart grids. *IEEE Power and Energy Society General Meeting*, 2014-October, 10 2014.
- [16] Shan Liu, Bo Chen, Takis Zourntos, Deepa Kundur, and Karen Butler-Purpy. A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, 5(3):1183–1195, 2014.
- [17] Ren Liu, Ceeman Vellaithurai, Saugata S. Biswas, Thoshitha T. Gamage, and Anurag K. Srivastava. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Trans Smart Grid*, 6(5):2444–2453, Sep 2015.
- [18] Mohamad El Hariri, Tarek Youssef, and Osama Mohammed. On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions? *Electronics*, 5(4):1–13, May 2016.
- [19] Chih Che Sun, Adam Hahn, and Chen Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56, 7 2018.
- [20] Chee Wooi Ten, Koji Yamashita, Zhiyuan Yang, Athanasios V. Vasilakos, and Andrew Ginter. Impact assessment of hypothesized cyberattacks on interconnected bulk power systems. *IEEE Transactions on Smart Grid*, 9:4405–4425, 9 2018.
- [21] Mohammadreza F.M. Arani, Amir Abiri Jahromi, Deepa Kundur, and Marthe Kasouf. Modeling and simulation of the aurora attack on microgrid point of common coupling. *7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2019 - Held as part of CPS Week, Proceedings*, 4 2019.
- [22] Amir Abiri Jahromi, Anthony Kemmeugne, Deepa Kundur, and Aboutaleb Haddadi. Cyber-physical attacks targeting communication-assisted protection schemes. *IEEE Transactions on Power Systems*, 35:440–450, 1 2020.
- [23] Norden E. Huang et al. The empirical mode decomposition and the Hubert spectrum for nonlinear and non-stationary time series analysis. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 454:903–995, 1998.
- [24] Ian Dobson and David E. Newman. Cascading blackout overall structure and some implications for sampling and mitigation. *International Journal of Electrical Power & Energy Systems*, 86:29–32, 3 2017.

- [25] Shinichi Imai, Damir Novosel, Daniel Karlsson, and Alexander Apostolov. Unexpected consequences: Global blackout experiences and preventive solutions. *IEEE Power and Energy Magazine*, 21:16–29, 5 2023.
- [26] Hyde M. Merrill, Md Abid Hossain, and Marc Bodson. Nipping blackouts in the bud: Introducing a novel cascading failure network. *IEEE Power and Energy Magazine*, 18:64–75, 7 2020.
- [27] Maedeh Mahzarnia, Mohsen Parsa Moghaddam, Payam Teimourzadeh Baboli, and Pierluigi Siano. A review of the measures to enhance power systems resilience. *IEEE Systems Journal*, 14:4059–4070, 9 2020.
- [28] Pouyan Pourbeik, Prabha S. Kundur, and Carson W. Taylor. The anatomy of a power grid blackout. *IEEE Power and Energy Magazine*, 4:22–29, 2006.
- [29] Ross Baldick et al. Initial review of methods for cascading failure analysis in electric power transmission systems. *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*, 2008.
- [30] Aliasghar Salehpour, Irfan Al-Anbagi, Kin Choong Yow, and Xiaolin Cheng. Modeling cascading failures in coupled smart grid networks. *IEEE Access*, 10:81054–81070, 2022.
- [31] Rounak Meyur, Anil Vullikanti, Madhav V. Marathe, Anamitra Pal, Mina Youssef, and Virgilio Centeno. Cascading effects of targeted attacks on the power grid. *Studies in Computational Intelligence*, 812:155–167, 2019.
- [32] Md Zahidul Islam, Yuzhang Lin, Vinod M. Vokkarane, and Venkatesh Venkataramanan. Cyber-physical cascading failure and resilience of power grid: A comprehensive review. *Frontiers in Energy Research*, 11:1095303, 2 2023.
- [33] Md Musabbir Hossain and Chen Peng. Cyber-physical security for on-going smart grid initiatives: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 5:233–244, 9 2020.
- [34] Mohammad Ghiasi, Taher Niknam, Zhanle Wang, Mehran Mehrandezh, Moslem Dehghani, and Noradin Ghadimi. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215:108975, 2 2023.
- [35] Luo Xu, Qinglai Guo, Yujie Sheng, S. M. Muyeen, and Hongbin Sun. On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. *Renewable and Sustainable Energy Reviews*, 152:111642, 12 2021.
- [36] Sandro Corsi and C. Sabelli. General blackout in italy sunday september 28, 2003, h. 03:28:00. *2004 IEEE Power Engineering Society General Meeting*, 2:1691–1701, 2004.

- [37] Shuva Paul, Fei Ding, Kumar Utkarsh, Weijia Liu, Mark J. O'Malley, and John Barnett. On vulnerability and resilience of cyber-physical power systems: A review. *IEEE Systems Journal*, 16:2367–2378, 6 2022.
- [38] Izhar Ahmed Khan, Dechang Pi, Nasrullah Khan, Zaheer Ullah Khan, Yasir Hus-sain, Asif Nawaz, and Farman Ali. A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. *Applied Intelligence*, 51:7306–7321, 10 2021.
- [39] Hang Zhang, Bo Liu, and Hongyu Wu. Smart grid cyber-physical attack and defense: A review. *IEEE Access*, 9:29641–29659, 2021.
- [40] Silvia Colabianchi, Francesco Costantino, Giulio Di Gravio, Fabio Nonino, and Riccardo Patriarca. Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, 160:107534, 10 2021.
- [41] Michael Abdelmalak, Venkatesh Venkataramanan, and Richard MacWan. A survey of cyber-physical power system modeling methods for future energy systems. *IEEE Access*, 10:99875–99896, 2022.
- [42] Andrew Clark and Saman Zonouz. Cyber-physical resilience: Definition and assessment metric. *IEEE Transactions on Smart Grid*, 10:1671–1684, 3 2019.
- [43] Lucas D. Valdez, Louis Shekhtman, Cristian E. la Rocca, Xin Zhang, Sergey V. Buldyrev, Paul A. Trunfio, Lidia A. Braunstein, and Shlomo Havlin. Cascading failures in complex networks. *Journal of Complex Networks*, 8, 4 2020.
- [44] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, and Lucian Mihet-Popa. Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access*, 8:151019–151064, 2020.
- [45] G. Andersson, P. Donalek, R. Farmer, N. Hatziaargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. Causes of the 2003 major grid blackouts in north america europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20:1922–1928, 11 2005.
- [46] Vaishali Rampurkar, Polgani Pentayya, Harivittal A. Mangalvedekar, and Faruk Kazi. Cascading failure analysis for indian power grid. *IEEE Transactions on Smart Grid*, 7:1951–1960, 7 2016.
- [47] Joshua Romero. Blackouts illuminate india's power problems. *IEEE Spectrum*, 49:11–12, 10 2012.
- [48] Diptak Pal, Balimidi Mallikarjuna, Pathirikkat Gopakumar, M. Jaya Bharata Reddy, Bijaya Ketan Panigrahi, and Dusmanta Kumar Mohanta. Probabilistic study of undervoltage load shedding scheme to mitigate the impact of protection system hidden failures. *IEEE Systems Journal*, 14:862–869, 3 2020.

- [49] A. M. Abdullah and K. Butler-Purry. Distance protection zone 3 misoperation during system wide cascading events: The problem and a survey of solutions. *Electric Power Systems Research*, 154:151–159, 1 2018.
- [50] Fangyu Li, Qi Li, Jinan Zhang, Jiabao Kou, Jin Ye, Wen Zhan Song, and Homer Alan Mantooth. Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network. *IEEE Transactions on Power Electronics*, 36:2495–2498, 3 2021.
- [51] P. Kundur and Om P. Malik. *Power system stability and control*. McGraw Hill Education, 2022.
- [52] M. A. Rahman, M. S. Rana, and H. R. Pota. Mitigation of frequency and voltage disruptions in smart grid during cyber-attack. *Journal of Control, Automation and Electrical Systems*, 31:412–421, 4 2020.
- [53] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi. Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. *IEEE Trans Power Systems*, 35(1):440–450, Jan 2020.
- [54] Abdallah Farraj, Eman Hammad, and Deepa Kundur. A cyber-physical control framework for transient stability in smart grids. *IEEE Transactions on Smart Grid*, 9:1205–1215, 2018.
- [55] Min Zhou, Chensheng Liu, Amir Abiri Jahromi, Deepa Kundur, Jing Wu, and Chengnian Long. Revealing vulnerability of n-1 secure power systems to coordinated cyber-physical attacks. *IEEE Transactions on Power Systems*, 38:1044–1057, 3 2023.
- [56] Yongdong Wu, Zhuo Wei, Jian Weng, Xin Li, and Robert H. Deng. Resonance attacks on load frequency control of smart grids. *IEEE Transactions on Smart Grid*, 9:4490–4502, 9 2018.
- [57] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In *Proceedings of the 33rd Annual Computer Security Applications Conference, ACSAC '17*, page 303–314, New York, NY, USA, 2017. Association for Computing Machinery.
- [58] Gururaghav Raman, Bedoor AlShebli, Marcin Waniek, Talal Rahwan, and Jimmy Chih Hsien Peng. How weaponizing disinformation can bring down a city’s power grid. *PLOS ONE*, 15:e0236517, 8 2020.
- [59] Mingxiao Ma and Abdelkader Lahmadi. On the impact of synchronization attacks on distributed and cooperative control in microgrid systems. *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2018*, 12 2018.
- [60] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 9:49–51, 5 2011.

- [61] Pengwei Du and Julia Matevosyan. Forecast system inertia condition and its impact to integrate more renewables. *IEEE Transactions on Smart Grid*, 9:1531–1533, 2018.
- [62] Anna Volkova, Michael Niedermeier, Robert Basmadjian, and Hermann De Meer. Security challenges in control network protocols: A survey. *IEEE Communications Surveys and Tutorials*, 21:619–639, 1 2019.
- [63] Shahbaz Hussain, Javier Hernandez Fernandez, Abdulla Khalid Al-Ali, and Abdulatif Shikfa. Vulnerabilities and countermeasures in electrical substations. *International Journal of Critical Infrastructure Protection*, 33:100406, 6 2021.
- [64] Debottam Mukherjee. Data-driven false data injection attack: A low-rank approach. *IEEE Transactions on Smart Grid*, 13:2479–2482, 5 2022.
- [65] Subhash Lakshminarayana, Abla Kammoun, Merouane Debbah, and H. Vincent Poor. Data-driven false data injection attacks against power grids: A random matrix approach. *IEEE Transactions on Smart Grid*, 12:635–646, 1 2021.
- [66] Vassilis C. Nikolaidis, Evangelos Papanikolaou, and Anastasia S. Safigianni. A communication-assisted overcurrent protection scheme for radial distribution systems with distributed generation. *IEEE Transactions on Smart Grid*, 7:114–123, 1 2016.
- [67] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li. Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems. *IEEE Trans Smart Grid*, 8(2):572–580, Mar 2017.
- [68] A. Ameli, A. Hooshyar, and E. F. El-Saadany. Development of a cyber-resilient line current differential relay. *IEEE Trans Industrial Informatics*, 15(1):305–318, Jan 2019.
- [69] J. Hong and C. Liu. Intelligent Electronic Devices With Collaborative Intrusion Detection Systems. *IEEE Trans Smart Grid*, 10(1):271–281, Jan 2019.
- [70] Mostafa Mohammadpourfard, Yang Weng, Abdullah Khalili, Istemihan Genc, Alireza Shefaei, and Behnam Mohammadi-Ivatloo. Cyber-physical attack conduction and detection in decentralized power systems. *IEEE Access*, 10:29277–29286, 2022.
- [71] J. Hoyos, M. Dehus, and T. X. Brown. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. In *in Proc 2012 IEEE Globecom Workshops*, pages 1508–1513, Anaheim, CA, Dec 2012.
- [72] T. A. Youssef, M. E. Hariri, N. Bugay, and O. A. Mohammed. IEC 61850: Technology standards and cyber-threats. In *Proc IEEE Int Conf on Environment and Electrical Engineering (EEEIC)*, pages 1–6, Florence, Jun 2016.
- [73] M. G. Kanabar and T. S. Sidhu. Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying. *IEEE Transactions on Power Delivery*, 26(2):725–735, Apr 2011.

- [74] Nishchal Kush, Ejaz Ahmed, Mark Branagan, and Ernest Foo. Poisoned GOOSE: Exploiting the GOOSE Protocol. In *Proc Australasian Information Security Conf*, pages 17–22, Auckland, Jan 2014.
- [75] Y. M. Khaw, A. A. Jahromi, A. Mohammadreza F. M., D. Kundur, S. Sanner, and M. Kassouf. Preventing false tripping cyberattacks against distance relays: A deep learning approach. In *Proc IEEE Int Conf on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–6, Beijing, Oct 2019.
- [76] Y. Yang, H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, and S. Sezer. Cybersecurity test-bed for IEC 61850 based smart substations. In *Proc IEEE Power Energy Society General Meeting*, pages 1–5, Denver, CO, Jul 2015.
- [77] M. Kabir-Querrec, S. Mocanu, J. Thiriet, and E. Savary. A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks. In *Proc IEEE Int Conf on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, Berlin, Sep 2016.
- [78] Omar Khaled, Andrés Marín, Florina Almenares, Patricia Arias, and Daniel Díaz. Analysis of Secure TCP/IP Profile in 61850 Based Substation Automation System for Smart Grids. *Int Journal of Distributed Sensor Networks*, 12(4):1–11, Apr 2016.
- [79] International Electrotechnical Commission. IEC 62351-6:2020 - Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850. <https://webstore.iec.ch/en/publication/63742>, 2020. Accessed: 2024-10-03.
- [80] S. M. Suhail Hussain. Lightweight Optimized Message Authentication Scheme for IEC 61850 Sampled Value Messages. *IEEE Transactions on Power Delivery*, pages 1–4, 2024.
- [81] S. M. Suhail Hussain, Shaik Mullapathi Farooq, and Taha Selim Ustun. A Method for Achieving Confidentiality and Integrity in IEC 61850 GOOSE Messages. *IEEE Transactions on Power Delivery*, 35:2565–2567, 10 2020.
- [82] Mikel Rodríguez, Jesús Lázaro, Unai Bidarte, Jaime Jiménez, and Armando Astarloa. A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems. *IEEE Access*, 9:51646–51658, 2021.
- [83] Nils Ole Tippenhauer, Binbin Chen, Daisuke Mashima, and David M. Nicol. vbump. In *Proceedings of the 2nd Workshop on CPS and IoT Security and Privacy*, pages 3–14. ACM, 11 2021.
- [84] Mohamed F. Elrawy, Camilla Fioravanti, Gabriele Oliva, Maria K. Michael, and Roberto Setola. A geometrical approach to enhance security against cyber attacks in digital substations. *IEEE Access*, 12:18724–18738, 2024.
- [85] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology — CRYPTO '96*, pages 1–15, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

- [86] Sizhe He, Yuxun Zhou, Yadong Zhou, Jiang Wu, Min Zheng, and Ting Liu. Fast identification of vulnerable set for cascading failure analysis in power grid. *IEEE Transactions on Industrial Informatics*, 19(4):5645–5655, 2023.
- [87] Pierre Henneaux et al. Benchmarking Quasi-Steady State Cascading Outage Analysis Methodologies. In *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, pages 1–6, 2018.
- [88] Jun Yan, Yufei Tang, Haibo He, and Yan Sun. Cascading failure analysis with dc power flow model and transient stability analysis. *IEEE Transactions on Power Systems*, 30(1):285–297, 2015.
- [89] Hale Cetinay, Saleh Soltan, Fernando A. Kuipers, Gil Zussman, and Piet Van Mieghem. Analyzing cascading failures in power grids under the ac and dc power flow models. *SIGMETRICS Perform. Eval. Rev.*, 45(3):198–203, March 2018.
- [90] Benjamin Schäfer, Dirk Witthaut, Marc Timme, and Vito Latora. Dynamically induced cascading failures in power grids. *Nature Communications*, 9:1975, 12 2018.
- [91] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thomas Lagkas, and Antonios G. Sariannidis. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys & Tutorials*, 22(3):1942–1976, 2020.
- [92] Rachad Atat, Muhammad Ismail, Shady S. Refaat, Erchin Serpedin, and Thomas Overbye. Cascading failure vulnerability analysis in interdependent power communication networks. *IEEE Systems Journal*, 16(3):3500–3511, 2022.
- [93] Rezoan Ahmed Shuvro, Pankaz Das, Jamir Shariar Jyoti, Joana M. Abreu, and Majeed M. Hayat. Data-integrity aware stochastic model for cascading failures in power grids. *IEEE Transactions on Power Systems*, 38(1):142–154, 2023.
- [94] Vetrivel Rajkumar, Marko Tealane, Alexandru Ștefanov, Alfian Presekal, and Peter Palensky. Cyber Attacks on Power System Automation and Protection and Impact Analysis. In *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pages 247–254, 2020.
- [95] Alfian Presekal et al. Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Transactions on Smart Grid*, 14(5):4007–4020, 2023.
- [96] Jiaxin Wu et al. Spectral graph clustering for intentional islanding operations in resilient hybrid energy systems. *IEEE Transactions on Industrial Informatics*, 19(4):5956–5964, 2023.
- [97] Ahad Esmaeilian and Mladen Kezunovic. Prevention of power grid blackouts using intentional islanding scheme. *IEEE Transactions on Industry Applications*, 53(1):622–629, 2017.
- [98] Morteza Dabbaghjamesh et al. A novel two-stage multi-layer constrained spectral clustering strategy for intentional islanding of power grids. *IEEE Transactions on Power Delivery*, 35(2):560–570, 2020.

- [99] Ilya Tyuryukanov et al. Controlled Power System Separation Using Generator PMU Data and System Kinetic Energy. *IEEE Transactions on Power Delivery*, 38(4):2618–2629, 2023.
- [100] Shuchismita Biswas et al. Proactive islanding of the power grid to mitigate high-impact low-frequency events. In *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, 2020.
- [101] Vetrivel Rajkumar, Alexandru Ștefanov, José Luis Rueda Torres, and Peter Palensky. Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks. *IEEE Transactions on Industrial Informatics*, 20(6):8807–8817, 2024.
- [102] Anton Tsitsulin et al. Graph clustering with graph neural networks. *Journal of Machine Learning Research*, 24(1), Mar 2024.
- [103] Simon J.D. Prince. *Understanding Deep Learning*. The MIT Press, 2023.
- [104] V. Rajkumar et al. Dynamical analysis of power system cascading failures caused by cyber attacks. *IEEE Transactions on Industrial Informatics*, 20(6):8807–8817, Mar 2024.
- [105] Mikel Rodríguez, Jesús Lázaro, Unai Bidarte, Jaime Jiménez, and Armando Astarloa. A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems. *IEEE Access*, 9:51646–51658, 2021.

