Formal Probabilistic Risk Assessment using Theorem Proving with Applications in Power Systems

Mohamed Wagdy Eldesouki Abdelghany

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy (Electrical and Computer Engineering) at

Concordia University

Montréal, Québec, Canada

September 2021

CONCORDIA UNIVERSITY

Division of Graduate Studies

This is to certify that the thesis prepared

By: **Mohamed Wagdy Eldesouki Abdelghany**

Entitled: **Formal Probabilistic Risk Assessment using Theorem Proving with Applications in Power Systems**

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy (Electrical and Computer Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

______________________ Prof. Alex De Visscher

______________________ Prof. Mark Lawford

______________________ Prof. Jun Yan

______________________ Prof. Luiz A. C. Lopes

______________________ Prof. Akshay Kumar Rathore

______________________ Prof. Sofiène Tahar

Approved by ______________________

Prof. Yousef R. Shayan, Chair of the ECE Department

August, 2021 ______________________

Prof. Mourad Debbabi, Dean, Faculty of Engineering and Computer Science

ABSTRACT

Formal Probabilistic Risk Assessment using Theorem Proving with Applications in Power Systems

Mohamed Wagdy Eldesouki Abdelghany, Ph.D.
Concordia University, 2021

The central inquiry in many safety-critical systems is to assess the probability of all possible risk consequences that can occur in a system and its subsystems. In this research, we use theorem proving to formalize Event Trees (ET), Cause Consequence Diagrams (CCD) and Functional Block Diagrams (FBD), which are efficient techniques for probabilistic risk assessment at system and subsystem levels. Our approach provides the reasoning support with verified mathematical formulations that can analyze multi-level ETs, FBDs for complex systems, Cause Consequence Diagrams (CCD) based on Fault Trees (FT) as well as on Reliability Block Diagrams (RBD), as a novel approach. Also, the proposed formalizations of ETs/CCDs/FBDs allowed us to accurately determine of reliability indices, such as System/Customer Average Interruption Frequency and Duration (SAIFI, SAIDI and CAIDI) at system and subsystem levels. Moreover, we develop FBD and ET Modeling and Analysis ($\mathbb{FETMA}$) software, which provides user-friendly features and graphical interfaces for industrial planners/designers. We applied our methods and tools on several realistic case studies from the power systems sector, i.e., the standard IEEE 3/39/118-bus electrical power generation/transmission/distribution networks, Québec-New England High Voltage Direct Current (HVDC) transmission coupling system, multiple interconnected Micro-Grids, a nuclear power plant, transmission distance protection and a smart automated substation. Experimental results showed improvements compared to all existing reliability analysis methods in terms of scalability, expressiveness, accuracy and time.

To my mother, father, brother and sisters,

To my rock and lovely wife.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the almighty god ALLAH.

Second, I sincerely thank my supervisor, Professor Sofiène Tahar, for giving me the opportunity to work on this multidisciplinary project on Formal Methods and Smart Grid Power Systems. Professor Tahar was always easily approachable, available and inspiring throughout the previous four years of my Ph.D. graduate studies. I have learned so much from his deep insights about research and strong expertise. I consider him not only as my supervisor but also as my second father.

Third, I would like to express my gratitude to Professor Mark Lawford for accepting to be my external Ph.D. thesis examiner and taking the time from his busy schedule to read and evaluate my doctoral thesis. My sincere gratitudes also go to Professors Jun Yan, Luiz A. C. Lopes and Akshay Kumar Rathore for serving on the advisory thesis committee during the past four years of my Ph.D. study, I deeply appreciate their great efforts.

Fourth, I would like to thank Dr. Waqar Ahmad for his help and advice while he was a postdoc in the HVG group as well as all my HVG friends Mubarka, Mahmoud, Seif, Yasmeen, Hassnaa, Sowimth and Abdelatif who made me feel welcomed by a family and their guidance offered when needed was generously overwhelming.

Finally, it gives me immense pleasure to thank my mother, father, brother and sisters, for their endless love and support. Nothing I say can do justice to how they feel about leaving them for years. Without their continuous support, this thesis would never start nor finish. My rock and lovely wife Reham, who has been with me in every moment of my Ph.D. tenure, is my source of strength and happiness. Her consistent love and encouragement kept me going till this point, and even farther. Her sacrifice by quitting her job and leaving her parents for years are not repayable nor forgettable.

TABLE OF CONTENTS

List of Tables

List of Figures

LIST OF ACRONYMS

AC	Alternating Current
ACR	Automatic Circuit Recloser
ASAI	Average Service Availability Index
ASCI	Average System Curtailment Index
ASUI	Average Service Unavailability Index
BB	Bus Bar
BCU	Bay Control Unit
BPU	Bay Protection Unit
BWR	Boiling Water Reactor
CAIFI	Customer Average Interruption Frequency Index
CAIDI	Customer Average Interruption Duration Index
CB	Circuit Breaker
CC	Complete Cylinder
CCD	Cause Consequence Diagram
CDF	Cumulative Distribution Function
CE	Conditional Event
CF	Complete Failure
CN	Customer Number
CORA	Continuous Reachability Analyzer
COPT	Capacity Outage Probability Table
CR	Cold Reserve
CS	Complete Success
CT	Current Transformer

CU	Control Unit
DC	Direct Current
DCCA	Deductive Cause Consequence Analysis
DPC	Direct Power Conversion
DS	Disconnecting Switch
EPN	Electrical Power Network
EI	Ethernet
EIR	Energy Index of Reliability
ENS	Energy Not Supplied Index
EPN	Electrical Power Network
ESS	Energy Storage Systems
ESW	Ethernet Switch
ET	Event Tree
ETMA	Event Tree Modeling and Analysis
F	Failure
FB	Functional Block
FBD	Functional Block Diagram
FETMA	Functional Block and Event Tree Modeling and Analysis
FMECA	Failure Modes, Effects, and Critically Analyses
FMR	Failure Mode Reasoning
FOL	First Order Logic
FOR	Forced Outage Rate
FT	Fault Trees
FTC	Fault Trip Circuit
G	Generator

GSC	Grid Side DC/AC Converter
GW	Gateway
HIPS	High-Integrity Protection Systems
HL	Hierarchical Level
HMI	Human Machine Interface
HOL	Higher Order Logic
HPCI	High Pressure Core Injection
HR	Hot Reserve
HVAC	High Voltage Alternating Current
HVDC	High Voltage Direct Current
IB	Inverter Bridge
IED	Intelligent Electronic Device
IM	Induction Motor
IPC	Industrial Personal Computer
LF	Line Filter
LOEE	Loss of Energy Expectation
LOLE	Loss of load Expectation
MC	Measuring Centers
MCC	Motor Control Center
MCS	Monte Carlo Simulation
MG	Micro Grid
MTTR	Mean Time to Repair
MU	Merging Unit
NCC	Network Control Center
OPF	Optimal Power Flow

P	Permanent Failure
PCS	Power Conversion System
PF	Partial Failure
PMU	Phasor Measurement Unit
PRA	Probabilistic Risk Assessment
PS	Power Supply
PT	Potential Transformer
PV	Photo-Voltaic
R	Protective Relay
RBD	Reliability Block Diagram
RCIC	Reactor Core Isolation Cooling
RES	Renewable Energy Resource
RHR	Residual Heat Removal
RSC	Rotor Side AC/DC Converter
S	Success
SA	Solar Array
SAS	Smart Automated Substation
SAIFI	System Average Interruption Frequency Index
SAIDI	System Average Interruption Duration Index
SCADA	Supervisory Control and Data Acquisition
SF	Steam Flow
SG	Smart Grid
SML	Standard Meta Language
SMV	Symbolic Model Checker
SPF	Semi Permanent Failure

SS	Subsystem
TA	Turbo Alternator
TF	Transient Failure
TC	Trip Circuit
TL	Transmission Line
TR	Transformer
TSO	Transmission System Operator
TTF	Time to Fail
TTR	Time to Repair
WT	Wind Turbine

Chapter 1

Introduction

In this chapter, we first introduce the motivation behind this doctoral thesis and the problem statement. Then, we present the most relevant related work, followed by our proposed methodology to achieve the goal of this doctoral research. Finally, we outline the main contributions achieved and the organization of this thesis.

1.1 Motivation

Probabilistic risk assessment (PRA) is a well-known comprehensive methodology for planners/designers to evaluate risks associated with safety-critical engineering systems [1]. In a PRA, there are four main steps for risk assessment: (1) risk identification; (2) risk and reliability analysis; (3) risk response plan; and (4) risk monitoring and control [2]. From the computation point of view, the second step is the most critical, where the risk is usually characterized by two main quantities: (i) the severity of the possible adverse consequence(s); and (ii) the likelihood of occurrence of each consequence. The likelihoods of risk consequences are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time), which can be determined through the reliability evaluation [3]. Therefore, the central safety inquiry in many complex systems to make decision-making at the critical design stage is to evaluate the probabilities of all possible risk consequences that can occur at system and subsystem levels using reliability modeling and analysis methods.

Reliability Modeling Methods

Since the late 60's, various types of reliability modeling methods have been developed to determine the probabilistic risk assessment of safety-critical systems. These include graph theory based approaches such as, Fault Trees (FT) [4], Reliability Block Diagrams (RBD) [5], Markov Chains [6] and Event Trees (ET) [7]. FTs mainly provide a graphical model for analyzing the factors causing a system failure only. On the other hand, RBDs provide a schematic structure for analyzing the success relationships of system components that keep the entire system reliable only. Markov Chains model the transition between working states and failure. ETs provide a risk tree model for all possible complete/partial failure and reliability consequence scenarios that can occur at the system-level simultaneously. Moreover, ET analysis can be used to associate failure and success events to all subsystems of a safety-critical system in more complex hierarchical structures, such as Functional Block Diagrams (FBD) [8]. An FBD is a graphical representation of the detailed system functionality and the functional relationship between all its subsystems that are represented as Functional Blocks (FB). More recently, an approach has been proposed to conduct ET analysis in conjunction with FTs to identify all subsystem failure events in a critical system and their cascading dependencies on the entire system. This analysis method is known as cause-consequence analysis, using a combined hierarchical structure of Cause-Consequence Diagrams (CCD) [9]. Therefore, the PRA of the occurrence of accident events using ETs/CCDs/FBDs can be used for all required system/subsystem-level improvements, thereupon, satisfy the reliability demand within acceptable risk levels.

Reliability Analysis Methods

The reliability analysis of safety-critical systems can be calculated using a variety of methods, among them analytically-based paper-and-pencil methods and simulation tools, such as Monte-Carlo, being the most popular [10]. The former one represents the system by a mathematical model and evaluate the reliability indices from this model manually. However, when realistic systems with complex operating procedures have to be modeled, the resulting analysis can therefore lose some of its significance due to the possibility of human error-proneness as well as to the very cumbersome effort to perform the reliability analysis manually. For that reason, many planners/designers use a simulation approach for faster computation, which uses random algorithms to predict the real functional behavior of safety-critical systems and estimate the average value of reliability parameters. On the other hand, *formal methods* [11], such as model checking, petri-nets and theorem proving, can be proposed as an accurate alternative to traditional analysis methods. Firstly, model checkers describe the behavior of systems in a state machine form and prove its characteristics in an accurate manner. However, model checkers suffer from the state space explosion problem [11]. Petri-nets is a mathematical modeling language, which is used for state-transition systems and describes the potential behavior of discrete systems in the form of states and transitions between states. However, Petri-nets are suffering from the reachability problem, which means it is not easy to determine when it is safe to stop [11]. Theorem proving uses a proof assistant to carry out mathematical proofs of theorems based on deductive reasoning and a set of basic axioms and inference rules at its core. The level of expressiveness of these theorems depends on the type of logic used, like first-order logic (FOL) and higher-order logic (HOL) [11].

1.2 State-of-the-Art

In this section, we present the existing state-of-the-art of ET and CCD/FBD reliability analysis at system and subsystem level, respectively.

Event Tree Reliability Analysis

Event Trees (ET) reliability analysis has been developed in the mid-70s' [7] for the probabilistic risk assessment of all possible sudden accident risks that can occur in nuclear power plants in the generation sector of power systems. Since that time, many researchers have analyzed safety-critical systems using ETs for the PRA at the design stage. For instance, Kennedy et al., in [12] used ET analysis to conduct the overall safety study of the Oyster Creek nuclear power plant in US for deducting all possible consequence scenarios of failure and reliability simultaneously. In the late 90s', Papazoglou in [13], was the first researcher to lay down the mathematical foundations of ETs to replace their graphical representation for probabilistic risk analysis of nuclear power plants. The mathematical analysis of ETs has been used in [14] to assess the probability of rare risk consequence events that can occur in power systems. In [15], Peplow et al. used an ET diagram to evaluate the probability of all possible consequences of sudden accident events or terrorist attacks causing the contamination with radioactive material, which would make a large surrounding area uninhabitable for thousands of years. Phulpin et al., in [16], used the ET analysis results to improve the control strategy of the High Voltage Direct Current (HVDC) transmission power flow and consequently the system sustainability aftermath of a large disturbance. Recently, Muzik et al., in [17], used the notion of ETs in analyzing all emergency risk possibilities of a Micro-Gird (MG) power system near the city of Pilsen, Czech Republic. However, the reliability analysis done in all the above-mentioned work is done purely analytically using a paper-and-pencil approach. A major limitation in the mathematical manual approach is the possibility of human error-proneness for large-scale realistic systems as well as the cumbersome effort and large amounts of time to perform the reliability analysis manually. On the other hand, there exist several commercial software tools for building ETs for probabilistic risk assessment of critical systems, such as Isograph [18], SoHAR [19], ReliaSoft [20] and ITEM [21]. These commercial tools require from the user to manually draw the ET model and only allow *two-states* for each component due to an explosion of outcome possible test cases, then compute the probability of each scenario by multiplying the probabilities of associated failure/success events in each scenario. The limitation of two-state models makes commercial ET analysis tools not suitable for realistic complex systems that usually require to assign *multi-states* of complete/partial failure and reliability events to each component. On the other hand, there are also simulation approaches for ET analysis that generally use random-based algorithms, such as MATLAB Monte-Carlo Simulation (MCS), to predict and estimate the probability of risk consequences [22]. These approximate simulation algorithms have been widely used in the reliability analysis of critical systems for faster computation. For instance, in [23] the authors used MCS based ET analysis to identify and evaluate the possible consequences of undesired events in railway tunnels. In [24], Yu et al. used ET-based MCS to implement the stochastic properties of contingencies, protective response and protection power system failures. However, MCS-based reliability analysis approaches lack the rigor of detailed proof steps for reliability analysis as well as require a large amount of computing time for large-scale systems due to an explosion of test cases [25].

Functional Block Diagram Reliability Analysis

In the late 90s', Papazoglou developed the fundamentals of FBD reliability analysis in [8], which recursively applies ET analysis for each subsystem of a safety-critical system and connect all subsystem-level ETs together in a hierarchical ET structure. FBD reliability analysis is mainly done using an analytically manual analysis approach. For instance, Papakonstantinou et al., in [26], used FBD analysis to determine all safety classes of a Boiling Water Reactor (BWR) and steam turbine generator in a nuclear power plant. Since that time, FBD analysis has not improved much due to the complexity that planners/designers are facing of building complex ET structure models manually during the design stage. A computer simulation program can be written in any modern language to automate the FBD analysis proposed by Papazoglou. However, both the manual and simulation methods either lack detailed proof steps and are not scalable for *multi-level* reliability analysis of realistic systems or use approximation algorithms for faster PRA computation. Therefore, these approaches could introduce undesirable inaccuracies that can be deemed fatal for safety-critical systems.

Cause Consequence Diagram Reliability Analysis

Cause Consequence Diagrams (CCD) reliability analysis was developed at the beginning of 2000's [9] to analyze failures at the subsystem levels using FTs combined with an ET consequence diagram to integrate their cascading failure/reliability dependencies on the entire system. CCDs are categorized into two general methods for the ET linking process with the FTs [9]: (1) Small ET diagram and large subsystem-level FT; (2) Large ET diagram and small subsystem-level FT. Both methods are used for the PRA of industrial applications. For example Andrews et al., in [27], used the former method of CCD reliability analysis (i.e., small ET and large FTs) to determine all the PRA of High-Integrity Protection Systems (HIPS). Also Andrews, in [28], used the latter approach (i.e., large ET and small FTs) to determine all possible complete/partial failure and reliability events at the subsystem level of a pressure tank system that contains a Motor Control Center (MCC) with a start-up and shutdown sequence in addition to its required operational phase. In [29], Vyzaite et al. applied both of the CCD method for reliability analysis of non-repairable critical-systems at each subsystem level. However, the subsystem-level CCD reliability analysis done in all the above-mentioned framework is done purely analytically based using a paper-and-pencil approach [9]. This raises a reliability research question, namely, how much time would be needed if planners/designers require *multi-level* cause consequence analysis corresponding to n-subsystems of a safety-critical system, i.e., *multi-level* ET model and *multi-level* FT models?

ET Reliability Analysis using Formal Methods

Only a few works have previously considered using formal methods for reliability analysis of safety-critical systems. For instance, Nỳvlt et al. in [30] used Petri nets for ET analysis to model the complete/partial system-level failure and success consequence events. The authors proposed a new method based on P-invariants to obtain a model of cascading dependencies in ETs [30]. However, according to the same authors, they are not able to obtain verified expressions from the generated ET model [30]. Ortmeier et al. in [31] developed a framework for Deductive Cause-Consequence Analysis (DCCA) using the SMV model checker [32] to verify the CCD proof obligations. However, according to the authors, there is a problem of showing the completeness of DCCA due to the exponential growth of the number of proof obligations with complex systems that need cumbersome proof efforts [31]. To the best of our knowledge, there exist no work applying formal methods for FBD reliability analysis.

1.3 Problem Statement

Existing reliability analysis methods for ETs/CCDs/FBDs compromise the accuracy or completeness of PRA during the critical design stage of safety-critical systems. The recommendations of international safety standards bodies, such as IEC 61850 [33], EN 50128 [34] and ISO 26262 [35], is to use formal methods for accurate PRA of realistic safety-critical systems. The developed frameworks for ETs and CCDs using formal methods, based on model checking and petri-nets, lack the ability to verify probabilistic expressions of all possible complete/partial failure and reliability consequence events that can occur simultaneously.

1.4 Proposed Solution

With the ultimate goal of accomplishing a rigorous ET/CCD/FBD reliability analysis of safety-critical systems that overcomes all above-mentioned limitations of existing analysis methods, we propose in this thesis to use formal methods, based on higher-order logic (HOL) theorem proving, for analyzing ETs, CCDs and FBDs. The reason for using an interactive theorem prover based on HOL rather than an FOL automated theorem prover is mainly due the capability of the former to reason about non-trivial probabilistic mathematical formulations needed for the reliability analysis efforts [36]. This would provide planners/designers the ability to obtain *formally verified* probabilistic consequence expressions of complete/partial failure and reliability at system and subsystem levels that model checking and petri-nets cannot sustain. There exist several HOL theorem provers that could be potential candidates for the anticipated research work, such as HOL4 [37], Isabelle [38], PVS [39], HOL-Light [40] and Coq [41], which vary in the availability of the supported libraries. In this doctoral thesis, we will use the HOL4 [37] theorem prover, which has a rich library of probability and measure theory as well as theories supporting reliability measures, such as those for FTs and RBDs. In fact, prior to this work, there were two notable projects for building formal infrastructures for reliability analysis in HOL4, which we briefly describe in the sequel.

Static Reliability Analysis in HOL4 In 2017, Ahmad [42] proposed a formal reliability analysis framework that uses HOL4 to analyze *multi-level* static FT and RBD structures. He first presented a higher-order-logic formalization of commonly used RBD configurations, namely, series, parallel and nested series-parallel, to facilitate the formal reliability analysis of safety-critical systems within the sound environment of the HOL4 theorem prover. Then, he developed the detailed formalization of commonly used FT gates, such as AND, OR, NOT, which are the foremost requirements to conduct FT analysis. The usability of the proposed FT/RBD formalization was effectively illustrated by presenting the formal reliability analysis of several realistic systems, including smart grids in HOL4. A limitation of the framework of [42] is that the formalization of the static RBDs and FTs can neither analyze the dynamic behavior of the critical system nor determine failure and reliability simultaneously.

Dynamic Reliability Analysis in HOL4 In 2019, Elderhalli [43] proposed a framework to formally conduct the dynamic dependability analysis of systems modeled as dynamic fault trees (DFTs) and dynamic reliability block diagrams (DRBDs) using HOL theorem proving. She formalized in HOL4 the DFT gates and operators, which enables having formally verified cut sets and cut sequences to qualitatively analyze a given DFT. She was able to report a flaw in one of the published DFT algebras, which further emphasize on the importance of formally validating the correctness reliability results of safety-critical systems. Moreover, she developed a novel DRBD algebra and introduced several operators and simplification theorems to mathematically model traditional RBD structures as well as the dynamic spare construct, which she formalized in HOL4. However, the framework of Elderhalli [43] can help designers/planners to analyze either dynamic failure or reliability only of a given safety-critical system.

Due to the limitations of existing formal framework in HOL4 for analyzing either failure or reliability for safety-critical systems, we propose the formalization of ETs in HOL4, which considers both failure and reliability states of safety-critical systems simultaneously. Also, we propose the formalization of CCDs, based on FT/RBD formalization in conjunction with the formalization of ETs to perform the subsystem level reliability analysis in HOL4. Moreover, we propose the formalization of FBDs in HOL4, which recursively applies the formalization of ETs for each subsystem of a complex safety-critical system. We use the formalization of ETS/CDDS/FBDs to evaluate different significant reliability and energy indices of realistic power grid applications at system and subsystem levels. Prior to this work, few researchers considered the use of formal methods to analyze the reliability of power systems.

Formal Reliability Analysis of Power Systems Mahmood et al., in [44], developed a framework for the reliability assessment of power grid components [45] with backup protection using the probabilistic model checker PRISM [11]. Similarly, in [46], Khurram et al. presented a foundational model for relay-based protected components in power distribution systems using the PRISM model checker. Also, in [47], Sugumar et al. were the first to used formal analysis via the UPPAAL model checker [48] to design and validate the Energy Management System (EMS) for a Micro-Grid (MG) system that consists of high penetration of solar PV systems. Also, Sugumar et al., in [25], used UPPAAL for the verification of a supervisory EMS, which provides much stronger confidence in the correctness of the EMS design than conventional approaches. Recently, Badings et al., in [49], used model checking for the predictive verification of smart power grids incorporating WTs and ESSs to overcome the need for sampling-based MCS and to be used by Transmission System Operator (TSO). However, all the above-mentioned model checking tools face a combinatorial blow up of the state-space, commonly known as the state explosion problem [11]. Moreover, in [50], Li et al. used the formal analysis, based on the continuous reachability analyzer (CORA) MATLAB toolbox [51], for the predictive verification of networked MG systems' stability in the presence of heterogeneous uncertainties induced by high penetration of RES generation. However, CORA has a limit of only providing probabilistic failure/reliability expressions of complex integrated MGs at each MG components level. Ahmad et al. in [52] used theorem proving to generate a Capacity Outage Probability Table (COPT) in order to estimate the overall capacity of the generation system. Also, Ahmad et al. in [53] used RBDs/FTs to determine either reliability or failure of various intelligent embedded devices for an automated substation.

1.5 Thesis Objective

The objective of the thesis is to develop methods and tools for the formal probabilistic risk assessment of multi-level complex systems with multi-state components of failure and reliability using theorem proving. This can be achieved through a rigorous methodology that can verify probabilistic expressions of realistic safety-critical systems at system and subsystem levels. To demonstrate the applicability of the proposed methodology, we applied the formal PRA to realistic applications in the power systems sector with the verification of significant reliability and energy indices.

1.6 Proposed Methodology

In this doctoral thesis, we propose a comprehensive framework for accurate and sound ET/FBD/CCD-based reliability analysis of large-scale critical systems using the HOL4 theorem prover. We propose new mathematical formulations that solve the state-of-the-art scalability problem of modeling *multi-level* ETs/CCDs/FBDs, which we formalized in HOL4. The verified probabilistic formulations in HOL4 are capable of analyzing multi-level systems, where each subsystem consists of components that are composed of *multi-states* failure and reliability events. The proposed formal analysis can be done on any arbitrary probabilistic distribution, like Exponential/Weibull/Poisson, which makes our framework the first of its kind. The core of the proposed framework are HOL4 theories for ETs, FBDs, and CCDs depicted in containers, as shown in Figure 1.1. During the critical system modeling and reliability analysis, industrial planners/designers usually require computer-aided visualization with graphical interfaces. For that purpose, we also develop an ET modeling and analysis software implemented in Python [54], called Functional Block Diagram and Event Tree Modeling and Analysis ($\mathbb{FETMA}$), as shown in Figure 1.1.

1. The ET theory consists of three parts: (1) *ET Structure*: we formalize in HOL4 the basic ET constructors for the mathematical modeling of ETs as well as functions for generating complex *multi-level* ET models; (2) *ET Reduction*: we formalize the ET reduction functions that can reduce the possible test cases of ETs based on the reliability requirements of the given safety-critical system; and (3) *Probabilistic Theorems*: we prove in HOL4 ET probabilistic theorems that are capable of analyzing complex ETs that consist of multiple *multi-state* system components and is based on any given probabilistic distribution and failure rates.

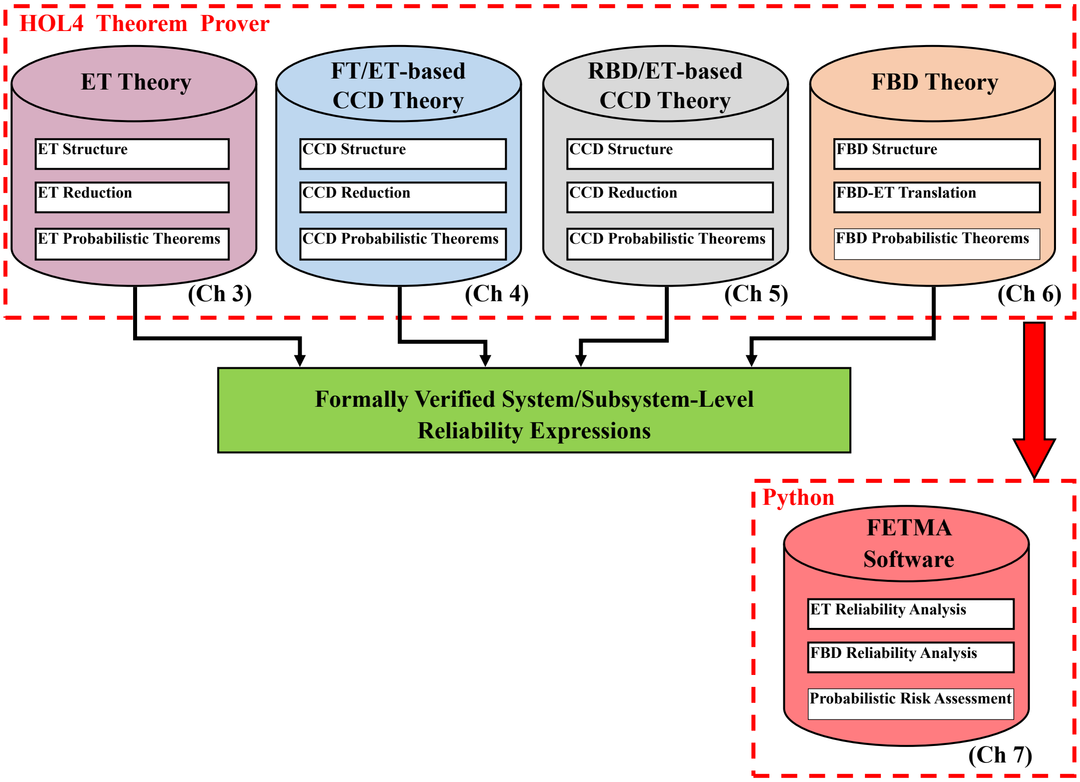


Figure 1.1: Proposed Methodology

2. The FT/ET-based CCD theory consists of three parts: (1) *CCD Structure*: we build in HOL4 the basic FT/ET-based CCD constructors for the mathematical modeling of CCDs and can express CCD models based on FTs and ETs; (2) *CCD Reduction*: we define a CCD reduction in HOL4 that can reduce the number of possible test cases of CCDs; and (3) *Probabilistic Theorems*: we prove FT/ET-based CCD probabilistic expressions in HOL4 that can perform failure analysis for *multi-level* subsystems of a complex system and obtain all possible failure and success consequence events at the subsystem level.

3. The RBD/ET-based CCD theory consists of three parts: (1) *CCD Structure*: we define in HOL4 the basic RBD/ET-based CCD constructors for the mathematical modeling of CCDs based on RBDs and ETs, as a novel approach; (2) *CCD*

Reduction: we formalize the CCD reduction in HOL4 that can reduce the number of possible test cases of CCDs; and (3) *Probabilistic Theorems*: we formalize novel RBD/ET-based CCD probabilistic theorems that can identify potential areas of poor reliability for *multi-level* subsystems of a complex system.

4. The FBD theory consists of three parts: (1) *FBD structure*: we formalize in HOL4 the basic FBD constructors for the mathematical modeling of FBDs; (2) *FBD-ET Translation*: we formalize in HOL4 a set of functions that can translate a complex FBD model to a hierarchical ET model; and (3) *Probabilistic Theorems*: we verify in HOL4 FBD probabilistic theorems to determine the probability of all consequence scenarios at the subsystem level that could occur in a complex system.

For industrial planners/designers, who usually require user-friendly features and graphical interfaces during the reliability analysis, we also implement in Python a Functional Block Diagram and Event Tree Modeling and Analysis ($\mathbb{FETMA}$) software that consists of three parts: (1) *ET Reliability Analysis*, which is based on the ET theory in HOL4; (2) *FBD Reliability Analysis*, which is based on the FBD theory in HOL4; (3) *Probabilistic Risk Assessment*, we evaluate in $\mathbb{FETMA}$ the probabilistic assessment of all possible consequence events at the system and subsystem levels.

Figure 1.2 depicts the process that would undertake for the probabilistic risk assessment of safety-critical systems using our formalizations of ETs, CCDs and FBDs in HOL4. The inputs to this process are the safety-critical system diagrams, descriptions, and subsystems' specifications provided by the reliability engineers. The second step is to choose which technique is suitable for the safety-critical system reliability analysis, i.e., using the ET option for system-level analysis or using either the FBD or CCD options for subsystem-level analysis, as shown in Figure 1.2.

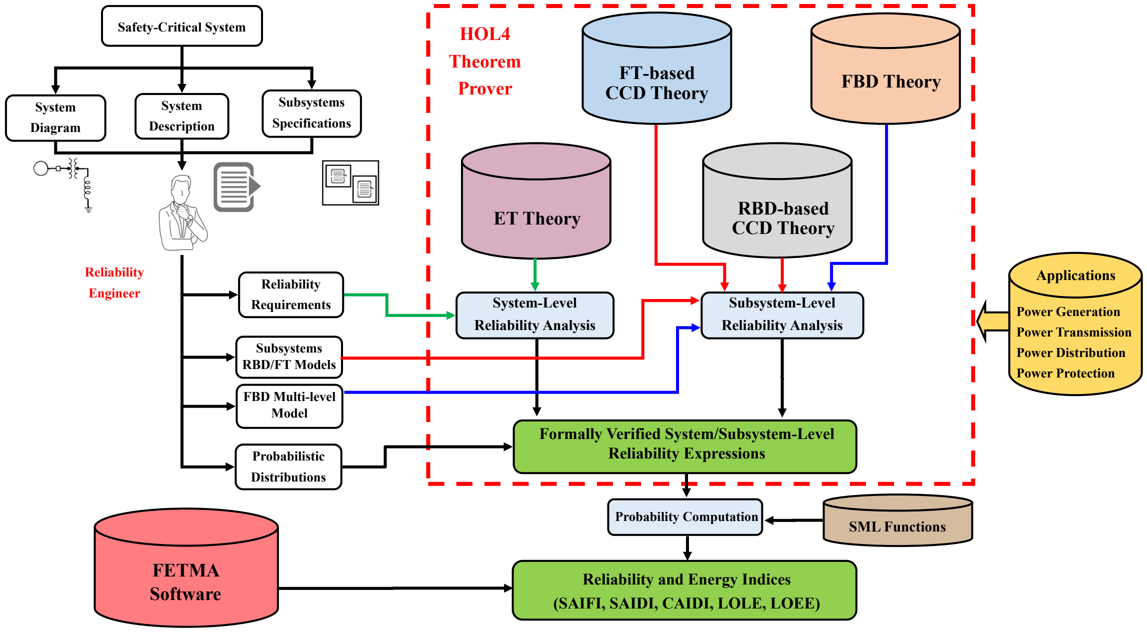


Figure 1.2: Formal Probabilistic Risk Assessment Process

To perform the formal system-level ET analysis using our ET theory, the reliability engineer has to provide the reliability requirements for the system under study, as shown in Figure 1.2 with green arrows. Similarly, using our CCD theories requires the subsystem RBD or FT models, as shown in Figure 1.2 with red arrows. The FBD theory requires the FBD multi-level model, as shown in Figure 1.2 with blue arrows. Based on our ET/FBD/CCD theories in HOL4, a designer/planner can easily verify all possible system/subsystem-level safety classes of complete/partial failure and reliability expressions based on any given probabilistic distribution, like Exponential/Weibull/Poisson, corresponding to the given system description. The last step is the computation of the formally verified risk consequence expressions using Standard Meta Language (SML) [55] functions. We can use the results to accurately determine significant reliability and energy indices, such as System/Customer Average Interruption Frequency/Duration Index (SAIFI, SAIDI and CAIDI) and Loss of load/Energy Expectation (LOLE and LOEE) [56], to help the planners/designers in making effective decisions at the critical design stage. In order to demonstrate the practical effectiveness of our proposed methodology, we use our framework to conduct a formal system/subsystem-level reliability analysis of realistic power systems in the four major power sectors [57]: (i) power generation plants; (ii) power transmission grids; (iii) power distribution networks; and (iv) power protection systems, as shown in Figure 1.2. We use different power system applications for different parts of our methodology in order to illustrate the usage of each technique for its suitable PRA. For example, ETs for PRA of large transmission systems that require system-level risk analysis, FT-based CCDs for PRA of conventional generation systems that usually require failure analysis at the subsystem level, RBD-based CCDs for PRA of renewable energy resources that are connected in series and parallel at subsystem levels and FBDs for PRA of nuclear power plants and substations that always require multi-level and multi-state risk analysis at the subsystem level. We assume that all failure rates are mutually independent and as future work, we will consider the dynamic behavior of failure rates as well as conditional probabilities.

1.7 Thesis Contributions

The main contribution of this thesis is the development of rigorous methods and tools for the formal system/subsystem-level probabilistic risk assessment of safety-critical systems. We list the contributions achieved in this thesis as follows. The publications cited are listed in the bibliography section provided at the end of the thesis document.

- Formalization of ET constructors in HOL4 that can be composed to build an arbitrary level of ET diagrams. Enabling formal ET-based probabilistic analysis in HOL4 with verified probabilistic formulations. Applications on three realistic power systems, i.e. IEEE 3-bus bulk power system, Québec-New England HVDC coupling between Canada and US and IEEE 118-bus power network.

[Bio-Jr1, Bio-Jr4, Bio-Cf3, Bio-Tr3]

- Formalization of the CCD basic constructors that can be used to build an arbitrary level of CCDs. Provide reasoning support for formal probabilistic analysis of *multi-level* CCDs, based on FTs and ETs. Application on a IEEE 39-bus generation network and verification of reliability indices at generation level.

  [Bio-Jr5, Bio-Tr1]

- Introduction of a novel approach to conduct CCD reliability analysis based on RBDs rather than FTs to identify potential areas of poor reliability. Formalization in HOL4 of newly developed probabilistic formulations of CCDs based on RBD and ET theories. Application on multiple interconnected micro-grids.

  [Bio-Jr3, Bio-Cf2]

- Formalization of FBDs by defining modeling functions for its basic elements. Provide reasoning support for formal probabilistic analysis of *multi-level* FBDs, which can mathematically analyze complex hierarchical ET structures. Application on a realistic nuclear power plant with multiple-levels decomposition of nuclear reactor, where we verified all possible safety classes that can occur.

  [Bio-Cf1]

- Development of a *Functional Block Diagram and Event Tree Modeling and Analysis* ($\mathbb{FETMA}$) software, which provides the probabilistic risk assessment of system/subsystem-level ET and FBD reliability analysis. Applications on a power transmission distance protection and a smart automated substation.

[Bio-Jr2, Bio-Cf5, Bio-Tr2]

1.8 Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2, is the preliminary chapter that summarizes the fundamentals of ET/CCD/FBD step-wise analysis and describes the basics of the HOL4 theorem prover. In Chapter 3, we describe our formalization of ETs in HOL4, i.e., ET modeling, ET reduction, ET partitioning, ET probabilistic analysis, ET reliability indices, and conduct different applications of two-state IEEE 3-bus bulk power system, multi-state Québec-New England HVDC system and two-state multiple ET models of IEEE 118-bus power network. In Chapter 4 we provide our formalization of FT/ET-based CCDs in HOL4, i.e., CCD modeling, CCD reduction, CCD partitioning, CCD probabilistic analysis, CCD reliability indices, and present a case study of the standard IEEE 39-bus distributed generation network system. In Chapter 5, we introduce a new RBD/ET-based cause consequence analysis approach with all required modeling and probabilistic formulations. We describe the formalization of this new RBD-based CCD method in HOL4 and provide an application on a four interconnected micro-grids of a smart power grid system. In Chapter 6, we provide our formalization of FBDs in HOL4, i.e., FBD modeling, FBD-ET translation, FBD probabilistic analysis, as well as an application on a realistic nuclear power plant generation system. In Chapter 7, we describe the internal structure of the $\mathbb{FETMA}$ software tool for system/subsystem-level ET and FBD reliability analysis, which are applied on a power transmission distance protection scheme and a smart automated substation. Lastly, Chapter 8 summarizes the contributions of this thesis and outlines potential future research directions.

Chapter 2

Preliminaries

In this chapter, we overview the basics of the methods used in this thesis for probabilistic risk assessment, namely, Event Trees (ET), Cause-Consequence Diagrams (CCD) and Functional Block Diagrams (FBD). We also introduce the fundamentals of the HOL4 theorem proving, the probability theory in HOL4 and the existing HOL4 theories of FTs and RBDs to facilitate the understanding of the rest of the thesis.

2.1 Event Trees

Event Tree (ET) [13] is a widely used probabilistic risk assessment technique that can analyze all possible system-level complete/partial failure and reliability consequence events by modeling components failure/success states simultaneously and determine their cascading dependencies on the entire system in the form of a tree structure. An ET diagram starts by an *Initiating Node* from which all possible consequence scenarios of a sudden event that can occur in the safety-critical system are drawn as *Branches* connected to *Proceeding Nodes* so that *only one* of these scenarios can occur, i.e., all possible ET consequence paths are mutually exclusive (cannot occur at the same

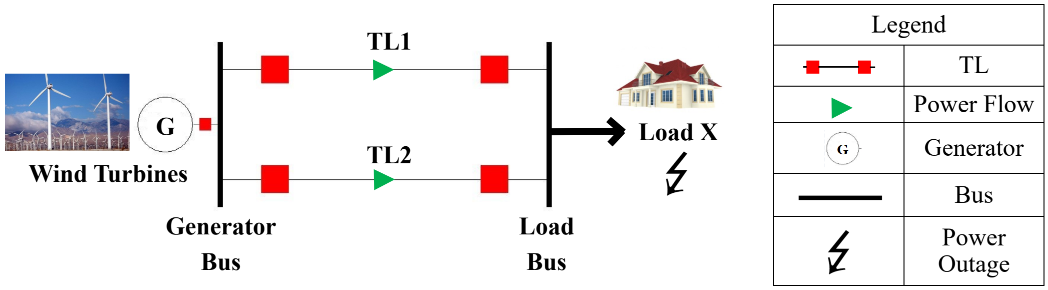
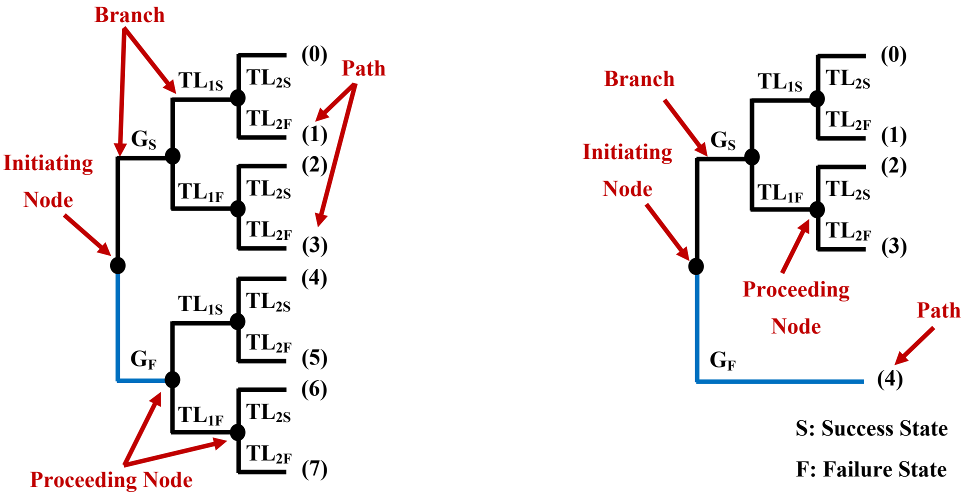


Figure 2.1: Schematic of an Example Micro-Grid System



(a) Complete Event Tree

(b) Reduced Event Tree

Figure 2.2: Micro-Grid System Event Tree Diagrams

instance) and distinct. For instance, consider a Micro-Grid system consisting of wind-turbines power generation (G) and two transmission lines (TL) to supply a certain load X, as shown in Figure 2.1. Assuming that each component in the Micro-Grid system has two operational states only, i.e., Success (S) state or Failure (F) state. The ET four steps analysis, introduced by Papazoglou [13], are as follows:

1. *Generation*: Construct a complete ET diagram that draws all possible scenarios, known as *Paths*. Each *path* consists of a unique sequence of failure/success events. Figure 2.2(a) depicts 8 ET consequence paths (from path 0 to path 7) with all possible scenarios that can occur in the Micro-Grid system.

2. *Reduction*: Model the accurate functional behavior of a system to reduce the number of possible test cases. This is done by deleting some specific nodes/branches corresponding to the occurrence of certain events, which are known as *Complete Cylinders* (CC) [13]. These cylinders are ET *paths* consisting of N failure/success events and are conditional on the occurrence of K *Conditional Events* (CE) in their respective paths. They are typically referred to as CCs with respect to K. For instance, if the wind turbine generation G fails, then the whole grid fails regardless of the next transmission line status, i.e., TL_1 and TL_2, as shown in Figure 2.2(b). The ET paths 4-7 are CCs with respect to G_F.

3. *Partitioning*: This step is essential as we are only interested in the occurrence of certain reliability/failure events according to the system safety requirements. For instance, suppose we are only focusing on the Complete Failure (CF) of the micro-grid, then the ET paths 3 and 4 are taken from the reduced ET. If we are analyzing the Partial Failure (PF) of the grid, then the ET paths 1 and 2 are considered while the grid Complete Success (CS) is only represented by path 0.

4. *Probabilistic analysis*: Lastly, evaluate the probabilities of ET paths based on the occurrence of an accident event in the system. These probabilities represent the likelihood of each scenario that can possibly occur in a entire system. If all events in an ET model are mutually independent, then the probability of any ET path can be computed by simply multiplying the individual probabilities of all failure and success events associated with the ET path [13]. For example, the probabilistic risk assessment of the micro-grid CS, PF and CF in Figure 2.1 can be expressed mathematically, respectively, as:

$$\begin{aligned}
Pr(\mathrm{Micro-Grid}_{CS}) &= Pr(\mathrm{G}_S) \times Pr(\mathrm{TL}_{1S}) \times Pr(\mathrm{TL}_{2S}) \\
Pr(\mathrm{Micro-Grid}_{PF}) &= Pr(\mathrm{G}_S) \times Pr(\mathrm{TL}_{1F}) \times Pr(\mathrm{TL}_{2S}) + \\
&\quad Pr(\mathrm{G}_S) \times Pr(\mathrm{TL}_{1S}) \times Pr(\mathrm{TL}_{2F}) \\
Pr(\mathrm{Micro-Grid}_{CF}) &= Pr(\mathrm{G}_S) \times Pr(\mathrm{TL}_{1F}) \times Pr(\mathrm{TL}_{2F}) + Pr(\mathrm{G}_F)
\end{aligned} \tag{2.1}$$

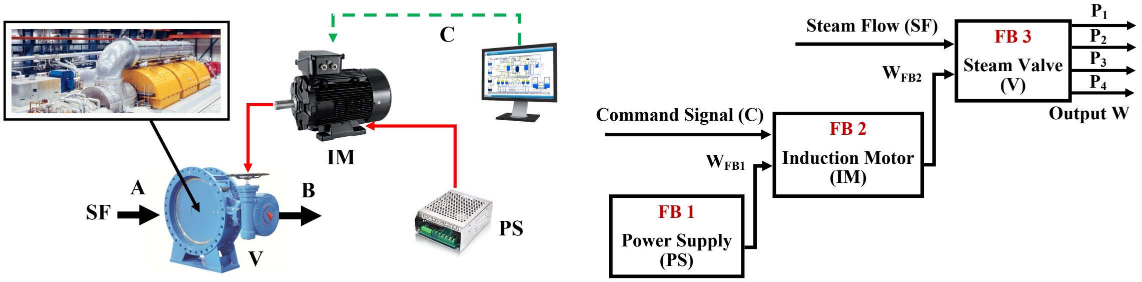
where $Pr(X_F)$ is the unreliability function or the probability of failure for a component X and $Pr(X_S)$ is the complement of $Pr(X_F)$ representing the reliability function or the probability of success of the component X, i.e. 1 - $Pr(X_F)$.

2.2 Functional Block Diagrams

Functional Block Diagram (FBD) [8] is an ET analysis based probabilistic risk assessment technique that can construct hierarchical ET structures to perform subsystem-level reliability analysis for complex systems. A Functional Block (FB) is the basic constructing element of an FBD graph that represents the stochastic behavior of each subsystem in a safety-critical system. To present a clear understanding of FBD-based safety analysis, consider a turbine governor system of a steam power plant that controls the position of a steam inlet valve (V), which in turn regulates the steam flow to the turbine and thus controls the output power. The valve operates with an induction motor (IM) that is energized by a power supply (PS), as shown in Figure 2.3(a). The main objective of the valve is to control the Steam Flow (SF) at point B given the flow situation at point A and a command signal C that dictates the required function of the valve, i.e. open or close. The FBD *six* step-wise analysis, are as follows:

1. *FBD Construction*: A system FBD (decomposed into FBs) is constructed based on the engineering knowledge to describe the subsystem-level behavior, as shown in Figure 2.3(b).

2. *ET Generation*: Construct a complete ET model corresponding to each subsystem FB. Assuming each subsystem component is represented by two operating states only, i..e, Success (S) or Fail (F). Figure 2.4 depicts the subsystem complete ETs, i.e., $ET_{1(\text{Complete})}$, $ET_{2(\text{Complete})}$ and $ET_{3(\text{Complete})}$ corresponding to FB_1, FB_2 and FB_3, respectively, of the steam-turbine governor.



(a) Steam-Turbine Governor System (b) FBD of Steam-Turbine Governor

Figure 2.3: Steam-Turbine Governor of a Thermal Power Plant

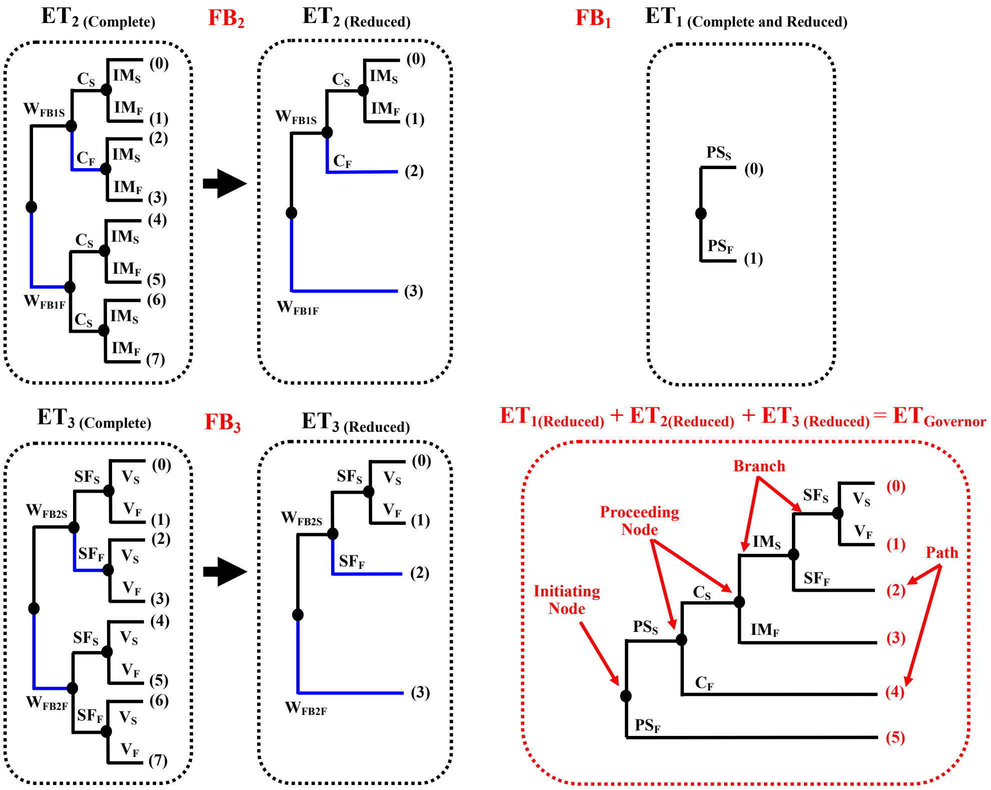

$ET_{2\ (\text{Complete})}$
FB_2
$ET_{2\ (\text{Reduced})}$
FB_1
$ET_{1\ (\text{Complete and Reduced})}$
W_{FB1S}
W_{FB1F}
C_S
C_F
IM_S
IM_F
PS_S
PS_F
(0)
(1)
(2)
(3)
(4)
(5)
(6)
(7)
$ET_{3\ (\text{Complete})}$
FB_3
$ET_{3\ (\text{Reduced})}$
W_{FB2S}
W_{FB2F}
SF_S
SF_F
V_S
V_F
$ET_{1(\text{Reduced})} + ET_{2(\text{Reduced})} + ET_{3\ (\text{Reduced})} = ET_{\text{Governor}}$
Branch
Proceeding Node
Initiating Node
Path

Figure 2.4: Steam-Turbine Governor ET Diagrams

3. *ET Reduction*: Obtain the reduced ETs by removing some nodes/branches according to subsystem functionality. For instance, in the steam-turbine governor FB_2 ($\text{ET}_{2(\text{Complete})}$), if the power supply FB_1 fails, then the whole IM fails regardless of the status of its other elements, as shown in Figure 2.4.

4. *ET Composition*: All reduced ETs are composed together considering the functional behavior of the steam-turbine governor system to form a complete subsystem-level ET model. So, $\text{ET}_{1(\text{Reduced})}$, $\text{ET}_{2(\text{Reduced})}$ and $\text{ET}_{3(\text{Reduced})}$ are composed to form a subsystem-level $\text{ET}_{\text{Governor}}$ (Figure 2.4) with all possible complete/partial failure and reliability ET consequence paths that can occur.

5. *ET Partitioning*: Safety analysts are usually interested in the occurrence of certain events according to the system safety requirements. For instance, suppose we are only focusing on the complete failure (CF) of the IM only in Figure 2.3(a), then ET paths 3-5 are obtained from $\text{ET}_{\text{Governor}}$.

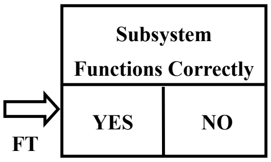
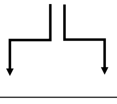
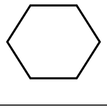
6. *Probabilistic Analysis*: This evaluates the probabilities of all possible safety classes of complete/partial failure and reliability subsystem-level ET paths based on the occurrence of a certain event in the entire system. For instance, the failure probability of IM_{CF} event in Figure 2.3(b) ($\text{ET}_{Path3-5}$) and the success probability of Governor_{CS} event (ET_{Path0}) can be expressed mathematically as:

$$\begin{aligned} &Pr(\text{IM}_{CF}) = Pr(\text{PS}_S) \times Pr(\text{C}_S) \times Pr(\text{IM}_F) + Pr(\text{PS}_S) \times Pr(\text{C}_F) \ + \ Pr(\text{PS}_F) \\ &Pr(\text{Governor}_{CS}) = Pr(\text{PS}_S) \times Pr(\text{C}_S) \times Pr(\text{IM}_S) \times Pr(\text{SF}_S) \times Pr(\text{V}_S) \end{aligned} \tag{2.2}$$

2.3 Cause Consequence Diagrams

Cause–Consequence Diagram (CCD) [9] is a probabilistic risk assessment technique that is traditionally used to model the causes of subsystem failures in a safety-critical system, using FT analysis, and their potential consequences on the entire system, using ET analysis [9]. The graph theory of CCDs uses three basic constructors *Decision box*, *Consequence path* and *Consequence box* [9]. The detailed description of the CCD constructors is illustrated in Table 2.1 [58]. To obtain a clear understanding of using FTs in CCDs, consider a renewable solar Photo-Voltaic (PV) energy system supplying a private house [59]. The PV system consists of two main subsystems: a Solar Array (SA) that consists of three series solar PV panels and an Inverter Bridge (IB) that converts DC to AC through Switches and Filters, as shown in Figure 2.5 [60]. The

Table 2.1: CCD Symbols and Functions

CCD Symbol	Function
	Decision Box: represents the status of functionality for a component or subsystem. (1) NO Box: describes the subsystem failure operation. An FT of the subsystem is connected to this box that can be used to obtain the failure probability, i.e., $Pr_{\text{NO}} = Pr_{\text{FT}}$ (2) YES Box: represents the correct functioning of the subsystem or reliability, which can be determined by simply taking the complement of the failure operation, i.e., $Pr_{\text{YES}} = 1 - Pr_{\text{FT}}$
	Consequence Path: models all possible consequence scenarios based on subsystem failure or reliability
	Consequence Box: models the final outcome due to a particular sequence of events for all subsystems

four steps of CCD analysis for the renewable energy solar PV system, as described by Andrews et al. [27], can be done as follows:

1. *Components failure events*: Assign an FT model to each subsystem in the solar system, i.e., FT$_{SA}$ (OR connection) and FT$_{IB}$ (OR connection).

$$\mathrm{FT_{SA}} = 1 - \Big(\big(1 - Pr(\mathrm{PV1}_F)\big) \times \big(1 - Pr(\mathrm{PV2}_F)\big) \times \big(1 - Pr(\mathrm{PV3}_F)\big) \Big) \quad (2.3)$$

$$\mathrm{FT_{IB}} = 1 - \Big(\big(1 - Pr(\mathrm{Switches}_F)\big) \times \big(1 - Pr(\mathrm{Filters}_F)\big) \Big) \quad (2.4)$$

2. *Construction of a complete CCD*: Draw a complete CCD model of the PV system, as shown in Figure 2.6(a). If the condition of the SA decision box is either YES or NO, then the next subsystem IB is taken into consideration. Each consequence path in the CCD analysis ends with either a PV system success (PV$_S$) or a PV failure (PV$_F$).

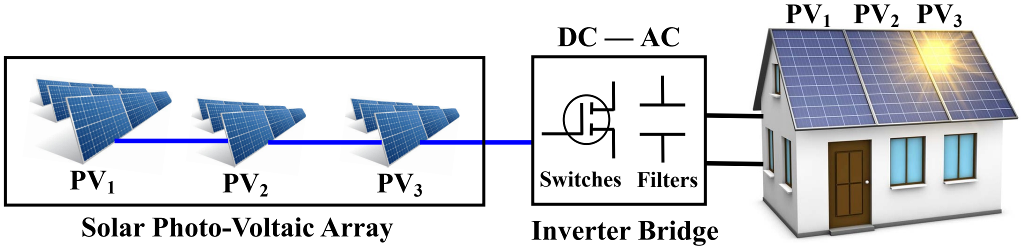
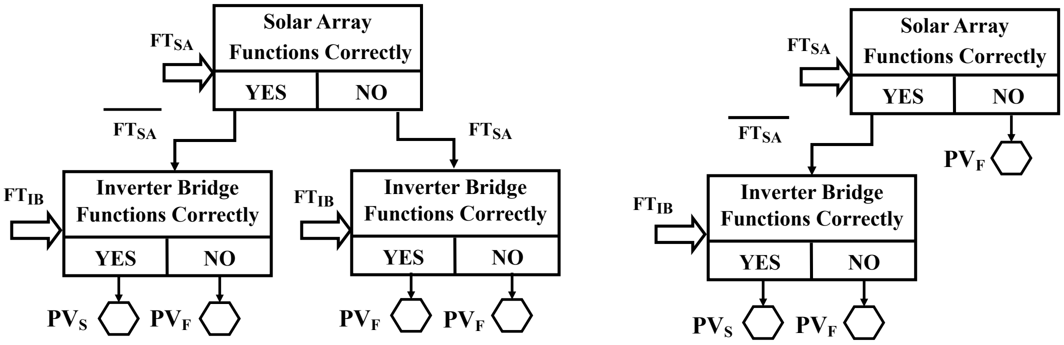


Figure 2.5: Solar Photo-Voltaic (PV) System



Solar Array Functions Correctly
FT$_{SA}$
YES
NO
$\overline{\mathrm{FT_{SA}}}$
FT$_{SA}$
FT$_{IB}$
Inverter Bridge Functions Correctly
YES
NO
PV$_S$
PV$_F$
FT$_{IB}$
Inverter Bridge Functions Correctly
YES
NO
PV$_F$
PV$_F$
Solar Array Functions Correctly
FT$_{SA}$
YES
NO
$\overline{\mathrm{FT_{SA}}}$
PV$_F$
FT$_{IB}$
Inverter Bridge Functions Correctly
YES
NO
PV$_S$
PV$_F$

(a) PV Complete CCD Model

(b) PV Reduced CCD Model

Figure 2.6: Photo-Voltaic Cause Consequence Analysis

3. *CCD model reduction*: Reduce the complete CCD model to decrease the number of test cases and model the accurate behavior of the PV system. If the condition of the SA decision box (SA functions correctly) is not satisfied, i.e., NO box, then the PV fails regardless of the status of the IB, as shown in Figure 2.6(b).

4. *CCD probabilistic analysis*: The probabilistic risk assessment of the two consequence boxes PV_S and PV_F at the subsystem level, as shown in Figure 2.6(b), can be expressed mathematically, using Equation 2.3 and Equation 2.4 as:

$$\begin{aligned} Pr\ (PV_S) = \; & Pr\ (\text{SA}_{\text{YES}}) \times Pr\ (\text{IB}_{\text{YES}}) = \\ & \Big(\big(1 - Pr(\text{PV1}_F)\big) \times \big(1 - Pr(\text{PV2}_F)\big) \times \big(1 - Pr(\text{PV3}_F)\big) \Big) \times \\ & \Big(\big(1 - Pr(\text{Switches}_F)\big) \times \big(1 - Pr(\text{Filters}_F)\big) \Big) \end{aligned} \tag{2.5}$$

$$\begin{aligned} Pr\ (PV_F) = \; & Pr\ (\text{SA}_{\text{YES}}) \times Pr\ (\text{IB}_{\text{NO}}) + Pr\ (\text{SA}_{\text{NO}}) = \\ & \Bigg(\Big(\big(1 - Pr(\text{PV1}_F)\big) \times \big(1 - Pr(\text{PV2}_F)\big) \times \big(1 - Pr(\text{PV3}_F)\big) \Big) \times \\ & \quad \Big(1 - \big(1 - Pr(\text{Switches}_F)\big) \times \big(1 - Pr(\text{Filters}_F)\big) \Big) \Bigg) + \\ & \Big(1 - \big(1 - Pr(\text{PV1}_F)\big) \times \big(1 - Pr(\text{PV2}_F)\big) \times \big(1 - Pr(\text{PV3}_F)\big) \Big) \end{aligned} \tag{2.6}$$

where $Pr(X_{NO})$ is the unreliability function or the probability of failure for a subsystem X, i.e., FT_X model, and $Pr(X_{YES})$ is the reliability function or the probability of operating, i.e., the complement of the FT_X model.

2.4 HOL4 Theorem Prover

The main characteristic of the HOL4 theorem prover is that its core consists only of four axioms and eight inference rules. Any further proof or theorem should be formally verified based on these axioms and rules or based on previously proven theorems. This ensures the soundness of the system model reliability analysis, i.e., no wrong proof goal can be proved. Table 2.2 provides the mathematical interpretations of some frequently used HOL4 symbols and defined functions, in this thesis. In the next subsection, we overview the measure and probability theory in the HOL4 theorem prover as well as the formalizations of FTs and RBDs in HOL4.

Table 2.2: HOL4 Symbols and Functions

HOL4 Symbols	Standard Symbol	Meaning
`{x	P(x)}`	$\{\lambda x.\ P(x)\}$	Set of all x that satisfy the condition $P(x)$
$L_1 :: L_N$	*cons*	List L_N of n elements $[L_1,\ L_2,\ L_3,\ L_4,\ \ldots, L_{n-1},\ L_n]$
λ`x. t`	$\lambda x.\ t$	Function that maps x to $t(x)$
`EL n` L_N	*element*	n^{th} element of list L_N
`exp x`	e^x	Exponential function
`prob p x`	*Pr (x)*	Probability of the event x
$\prod\ (X_1 :: X_N)$	$\prod_{i=1}^{N} X_i$	Product of the elements of a list X_N, i.e., $X_1 \times X_2 \times X_3 \times X_4 \times \cdots \times X_{n-1} \times X_n$
$\sum\ (Y_1 :: Y_N)$	$\sum_{i=1}^{N} Y_i$	Sum of the elements of a list Y_N, i.e., $Y_1 + Y_2 + Y_3 + Y_4 + \cdots + Y_{n-1} + Y_n$
$\mathrm{Pr_L}\ (Z_1 :: Z_N)$	*Probability list*	Probabilities of the elements of a list Z_N, i.e., $[Pr(Z_1), Pr(Z_2),,\ \ldots, Pr(Z_n)]$
`COMPL_LIST` $(H_1 :: H_N)$	*Complement list*	Complement of the elements of a list H_N, i.e., $[(1 - H_1), (1 - H_2), \ldots, (1 - H_n)]$

Measure and Probability Theory in HOL4

Measure space is defined mathematically as a triple (Ω, Σ, and μ), where Ω represents the sample space, Σ represents a σ-algebra of subsets of Ω, and μ represents a measure with the domain Σ. A probability space is a measure space (Ω, Σ, and Pr), where Ω is the complete sample space, Σ is the corresponding event space containing all failure/success events of interest, and Pr is the probability measure of the sample space as 1. The HOL4 theorem prover has a rich library of probabilities, including the basic probabilistic functions `p_space`, `events` and `prob` [61]. Given a probability space p, i.e., `p_space p`, `events p` and `prob p`, these functions return the corresponding probability space Ω, Σ, and Pr, respectively. The Cumulative Distribution Function (CDF) or failure function is defined as the probability of the failure event over certain interval of time t, where a random variable X has a value less or equal to a value t, i.e., $Pr\ (X \leq t)$. This definition can be been formalized in HOL4 as [61]:

Definition 2.1.

```
⊢ CDF p X t = distribution p X {y | y ≤ t}
```

where the function `CDF` takes three inputs: (i) a probability space p; (ii) a variable X; and (iii) a certain time t, then applies the function `distribution`, which returns the probability of the variable X acquiring all the values less than or equal the given specific time t in the probability space p. Similarly, reliability *R(t)* is stated as the probability of a system or component performing its desired task over time t.

$$R(t) = Pr\ (X > t) = 1 - Pr\ (X \leq t) = 1 - F_X(t) \tag{2.7}$$

where $F_X(t)$ is the CDF. The reliability function is defined as the probability of a system performing its desired task over time t, i.e., $Pr\ (X > t)$, in HOL4 as [42]:

Definition 2.2.

```
⊢ Reliability p X t = 1 - CDF p X t = distribution p X {y | y > t}
```

where each function `Reliability` takes the same three inputs as Definition 2.1 and returns the probability of the random variable X acquiring all the values greater than a specific time t in the probability space p. In the application sections of this thesis, we will assume that the failure CDF and reliability states of all safety-critical system/subsystem components are continuous exponentially distributed [62]. The exponential probabilistic distribution is well-known as *memoryless* and is routinely used in the reliability analysis of real-world systems to determine probability of failure (Pr (X $\leq$ t)) and probability of success (Pr (X > t)) for each system component over a time period t of interest as follows:

1. `CDF p X t = 1 -` $e^{(-\lambda_X t)}$
2. `Reliability p X t =` $e^{(-\lambda_X t)}$

where λ_X is the failure rate of the component X.

FT Formalization in HOL4

Fault Tree (FT) analysis [63] mainly provides a schematic diagram, using *logic*-gates, like OR, AND and NOT, for analyzing undesired *top events*, which can cause complete subsystem failure upon their occurrence. The failure probability expression of the AND FT gate at a specific time t, can be expressed mathematically as [63]:

$$\mathcal{F}_{AND_{Gate}}(t) = Pr\left(\bigcap_{i=1}^{J} F_i(t)\right) = \prod_{i=1}^{J} \mathcal{F}_i(t) \tag{2.8}$$

Similarly, the failure probability expression of the OR FT gate at a specific time t, can be expressed mathematically as [63]:

$$\mathcal{F}_{OR_{Gate}}(t) = Pr\left(\bigcup_{i=1}^{K} F_i(t)\right) = 1 - \prod_{i=1}^{K}(1 - \mathcal{F}_i(t)) \tag{2.9}$$

Ahmad [42] presented the formalization of FT in HOL4 by defining a new datatype gate, as follows:

Hol_datatype `gate = AND of (gate list) | OR of (gate list) |`

`NOT of (gate) | atomic of (event)`

The FT constructors `AND` and `OR` are recursive functions on `gate`-typed lists, while the FT constructor `NOT` operates on a `gate`-type variable. A semantic function is then defined over the `gate` datatype that can yield an FT diagram as [42]:

Definition 2.3. *Fault Tree*

⊢ `FTree p (atomic` F_X`) =` F_X $\wedge$

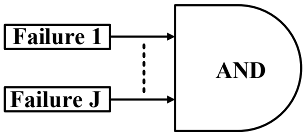
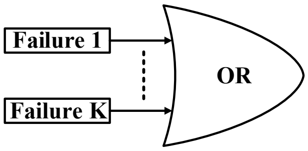
`FTree p (OR  (`F_1`::`F_J`)) = FTree p` F_1 $\cup$ `FTree p (OR ` F_J`)` $\wedge$

`FTree p (AND (`F_1`::`F_K`)) = FTree p` F_1 $\cap$ `FTree p (AND` F_K`)` $\wedge$

`FTree p (NOT` F_X`) = p_space p DIFF FTree p` F_X

The function `FTree` takes a failure event `X`, identified by `atomic`, and returns the given failure event `X`. If the function `FTree` takes a list F_J of J failure events, identified by `OR`, then it returns the union of all elements after applying the function `FTree` on each element of the given list. Similarly, if the function `FTree` takes a list F_K of K failure events, identified by `AND`, then it performs the intersection of all elements after applying the function `FTree` on each element of the given list. For the `NOT` type constructor, the function `FTree` returns the complement of the failure event obtained from the function `FTree` in the given probability space p. The formal formulation in HOL4 for the FT gates AND and OR probabilistic expressions Equation 2.8 and Equation 2.9, respectively, is presented in Table 2.3 [42]. The functions $\prod$, $\mathrm{Pr_L}$ and

Table 2.3: FT HOL4 Probabilistic Theorems

FT Gate	Probabilistic Theorem
	$\vdash \texttt{prob p (FTree p (AND } \mathrm{F}_J\texttt{)) =}$ $\prod \texttt{(}\mathrm{Pr_L}\texttt{ p } \mathrm{F}_J\texttt{)}$
	$\vdash \texttt{prob p (FTree p (OR } \mathrm{F}_K\texttt{)) =}$ $\texttt{1 - } \prod \texttt{(}\mathrm{Pr_L}\texttt{ p (COMPL\_LIST p } \mathrm{F}_K\texttt{))}$

COMPL_LIST are described in Table 2.2 [42]. These FT probabilistic expressions are verified under the following constraints: (a) `events p` ensures that all associated failure events are drawn from the events space p; (b) `prob_space p` ensures that p is a valid probability space; and lastly (c) MUTUAL_INDEP ensures the independence of the associated events, i.e., an event list E_N of N failure events are mutual independent if and only if for each subset k events, such that $(1 < k < N)$, we have:

$$Pr\left(\bigcap_{i=1}^{k} E_i\right) = \prod_{i=1}^{k} Pr(E_i) \tag{2.10}$$

The above mutual independent has been formalized in HOL4 as follows [42]:

Definition 2.4. *Mutual Independence of Events*

$\vdash \texttt{MUTUAL\_INDEP p } \mathrm{E}_N$

$\Leftrightarrow \texttt{prob p } \big(\bigcap \texttt{ p (TAKE k } \mathrm{E}_N\texttt{)}\big) \texttt{ = } \prod \big(\mathrm{Pr_L}\texttt{ p (TAKE k } \mathrm{E}_N\texttt{)}\big)$

where the function TAKE takes any k events from the event list E_N.

RBD Formalization in HOL4

A Reliability Block Diagram (RBD) [64] mainly provides a schematic diagram, using *series* and *parallel* configurations, for analyzing the success relationships of subsystem components that keep the entire subsystem reliable. The reliability of a subsystem when its components are connected in series configuration can be expressed as [64]:

$$\mathcal{R}_{series}(t) = Pr\left(\bigcap_{i=1}^{J} R_i(t)\right) = \prod_{i=1}^{J} \mathcal{R}_i(t) \tag{2.11}$$

Similarly, the reliability of a subsystem where its components are connected in parallel can be mathematically expressed as [64]:

$$\mathcal{R}_{parallel}(t) = Pr\left(\bigcup_{i=1}^{K} R_i(t)\right) = 1 - \prod_{i=1}^{K}(1 - \mathcal{R}_i(t)) \tag{2.12}$$

Ahmad in [42] developed the formalization of RBDs in HOL4 by defining a new datatype, as follows:

Hol_datatype `rbd = series of (rbd list) | parallel of (rbd list) |`

```
                   atomic of (event)
```

A semantic function is then defined over the `rbd` datatype that can yield mathematically the corresponding RBD diagram as [42]:

Definition 2.5. *Reliability Block Diagrams*

⊢ `rbd_struct p (atomic` R_X`) =` R_X $\wedge$

`rbd_struct p (series (`R_1`::`R_J`)) =`

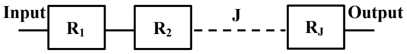
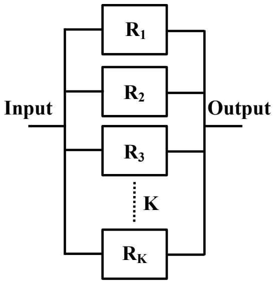
`rbd_struct p` R_1 $\cap$ `rbd_struct p (series` R_J`)` $\wedge$

`rbd_struct p (parallel (`R_1`::`R_K`)) =`

`rbd_struct p` R_1 $\cup$ `rbd_struct p (parallel` R_K`)`

The function `rbd_struct` takes a single event `X`, identified by a basic type constructor `atomic`, and returns the given event `X`. If the function `rbd_struct` takes an arbitrary list R_J of type `rbd`, identified by a type constructor `series`, then it performs the intersection of all J elements after applying the function `rbd_struct` on each element of the given list. Similarly, if the function `rbd_struct` takes an arbitrary list R_K of type `rbd`, identified by a type constructor `parallel`, then it returns the union of all K elements after applying the function `rbd_struct` on each element of the list. The formal formulations in HOL4 for the reliability series and parallel probabilistic expressions Equation 2.11 and Equation 2.12, respectively, is presented in Table 2.4 [42]. The functions $\prod$, Pr_{L}, `COMPL_LIST` are defined in Table 2.2.

Table 2.4: RBD Probabilistic Theorems

RBD Connection	Probabilistic Theorem
	$\vdash$ `prob p (rbd_struct p (series` R_J`)) =` $\prod$ `(`Pr_{L} `p` R_J`)`
	$\vdash$ `prob p (rbd_struct p (parallel` R_K`)) =` `1 -` $\prod$ `(`Pr_{L} `p (COMPL_LIST p` R_K`))`

Chapter 3

Formal Event Tree Reliability Analysis

In this chapter, we provide the detailed formalization of ET constructs and analysis steps described in the previous chapter, namely, ET modeling, ET reduction, ET partitioning and ET probabilistic analysis. Then, we describe a formal ET analysis process and define several reliability indices in HOL4, which we apply on different levels of realistic ET models of electrical power grids.

3.1 ET Formalization

3.1.1 Formal ET Modeling

We start the formal modeling of ETs by developing a new ET datatype in HOL4 as:

```
Hol_datatype EVENT_TREE = ATOMIC of (event) |
                          NODE of (EVENT_TREE list) |
                          BRANCH of (event) (EVENT_TREE)
```

The new datatype `EVENT_TREE` consists of three basic ET constructors `ATOMIC`, `NODE` and `BRANCH` corresponding to a single event, node and branch, respectively. The basic ET constructor `ATOMIC` takes a single event while the basic ET constructor `NODE` takes a recursive `EVENT_TREE`-typed list and lastly the basic ET constructor `BRANCH` takes an event and a recursive `EVENT_TREE`-typed. A semantic function is then defined that can yield a corresponding ET diagram as:

Definition 3.1. *Event Tree*

$\vdash$ `ETREE (ATOMIC` E_X`) =` E_X $\wedge$

`ETREE (NODE (`E_1`::`E_J`)) = ETREE` E_1 $\cup$ `(ETREE (NODE` E_J`))` $\wedge$

`ETREE (BRANCH` E_X ET_Y`) =` E_X $\cap$ `ETREE` ET_Y

If the function `ETREE` takes a success/fail event E_X, identified by `ATOMIC`, then it returns the event E_X. If the function `ETREE` takes a list (E_1::E_J), identified by `NODE`, then it returns the union of all the list's events. Similarly, if the function `ETREE` takes an event E_X and a proceeding event tree ET_Y, identified by `BRANCH`, then it performs the intersection of the event E_X with the next ET model ET_Y. Moreover, we define a *generic* function ET_{PATH} in HOL4 to obtain a specific path in the ET model. This was done in HOL4 by using the HOL4 recursive function `FOLDL` that takes three inputs: (1) a function that is recursively applied on the list elements (`BRANCH`); (2) the first success/fail branch event E_1; and (3) a list of different $\mathcal{N}$ events $\mathrm{E}_\mathcal{N}$, as follows:

Definition 3.2. *ET Path of* $\mathcal{N}$ *Events*

$\vdash$ ET_{PATH} `p (`E_1`::`$\mathrm{E}_\mathcal{N}$`) = FOLDL (`λ` a b. ETREE (BRANCH a b))` E_1 $\mathrm{E}_\mathcal{N}$

Now, we endeavor to formally define a generic function that can generate a large-scale ET model consisting of $\mathcal{N}$ components of a given system and each component is represented by a different $\mathcal{M}$ *multi-state* model for reliability studies (i.e., two-state model, three-state model, ..., $\mathcal{M}$-state model), as shown in Figure 3.1. The figure depicts examples of two-state (up and down), three-state (up, down and partly), four-state (in service, reserve shutdown, forced out in period of use and forced out but not used) and five-state models (failed, in service, hot reserve, cold reserve and fail to take up load). We start by defining a function $\bigotimes_{\mathrm{L}}$ that can model an ET diagram with all possible scenarios for two node lists, as shown in Figure 3.2(a), based on the mathematical Cartesian product $\bigotimes$ concept, in HOL4 as:

Definition 3.3. *Two Stair ET Generation*

$\vdash \mathrm{L}_1 \bigotimes_{\mathrm{L}} \mathrm{L}_2$ = `MAP (`λ` a. MAP (`λ` b. ETREE (BRANCH a b)) `L_2`)` L_1

Now, we can define a generic function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ that takes an arbitrary list of $\mathcal{N}$ components and generates a corresponding complex ET model with all possible scenarios

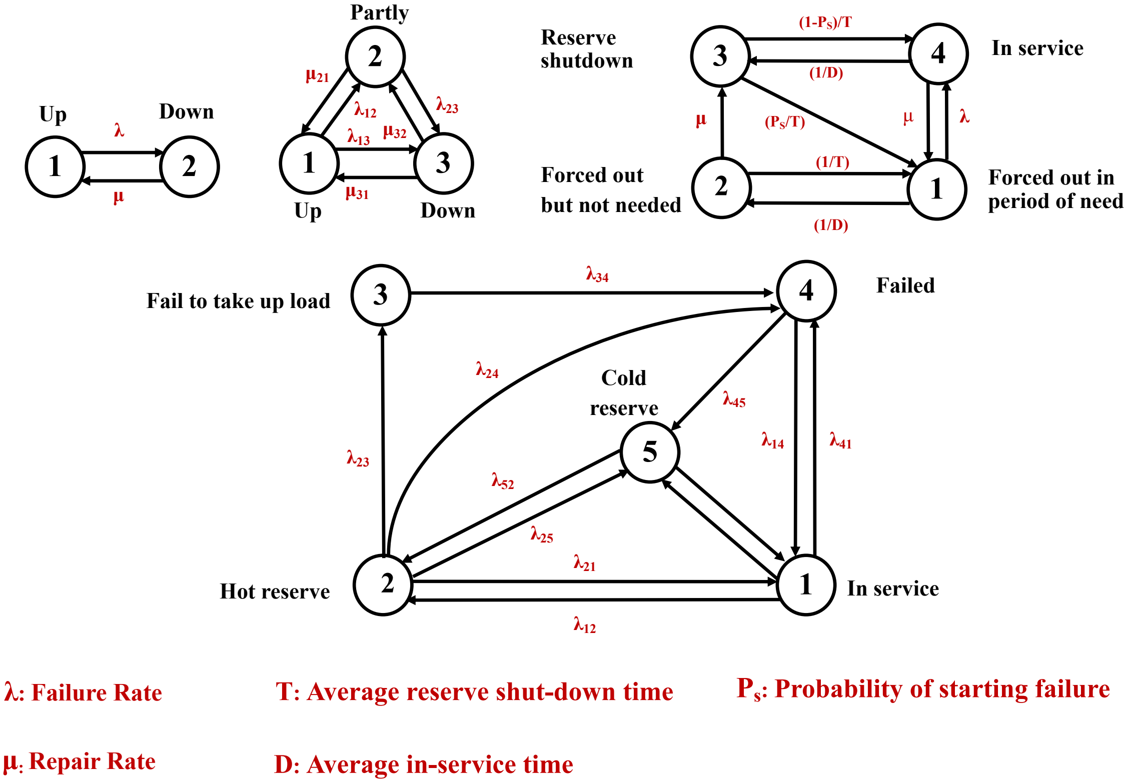
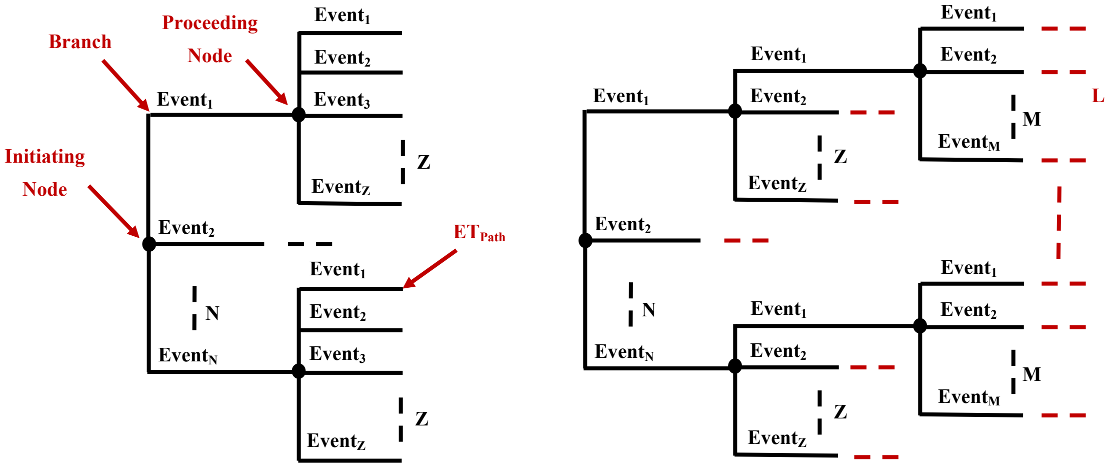


Figure 3.1: Multi-State Models for Reliability Studies



(a) Two Stair ET Generation

(b) $\mathcal{N}$ Stair ET Generation

Figure 3.2: Generic ET Model Generation

(i.e., $\mathcal{C}_1 \bigotimes \mathcal{C}_2 \bigotimes \cdots \bigotimes \mathcal{C}_{\mathcal{N}-1} \bigotimes \mathcal{C}_{\mathcal{N}}$), as shown in Figure 3.2(b), in HOL4 as:

Definition 3.4. *$\mathcal{N}$ Stair ET Generation*

$\vdash$ L $\bigotimes_{\text{L}}^{\mathcal{N}}$ $\text{L}_{\mathcal{N}}$ = FOLDR (λL_1 L_2. L_1 $\bigotimes_{\text{L}}$ L_2) $\text{L}_{\mathcal{N}}$ L

where L is a *list* of all given component states till $\mathcal{N}-1$ (i.e., $\text{L} = [[\mathcal{C}_1]; [\mathcal{C}_2];\ldots; [\mathcal{C}_{\mathcal{N}-1}]]$) and $\text{L}_{\mathcal{N}} = [\mathcal{C}_{\mathcal{N}}]$. For instance, we can define the sequential complete ET model for the Micro-Grid system shown in Figure 2.2(a) with all possible complete/partial reliability and failure consequence events (8 test cases), mathematically in HOL4 as:

Definition 3.5. *Micro-Grid Complete ET Model*

$\vdash$ MicroGrid_Complete_ET [[G_S;G_F]; [TL_{1S};TL_{1F}]; [TL_{2S};TL_{2F}]] =

ETREE $\big($NODE ([[G_S;G_F]; [TL_{1S};TL_{1F}]] $\bigotimes_{\text{L}}^{\mathcal{N}}$ [TL_{2S};TL_{2F}]$\big)$

We can formally verify the generated sequential complete ET mathematical model of the Micro-Grid system corresponding to Figure 2.2(a), in HOL4 as follows:

Theorem 3.1. *Verification of the Micro-Grid Complete ET Model*

$\vdash$ MicroGrid_Complete_ET [[G_S;G_F]; [TL_{1S};TL_{1F}]; [TL_{2S};TL_{2F}]] =

ETREE $\big($NODE [BRANCH G_S (NODE [BRANCH TL_{1S} (NODE [TL_{2S};TL_{2F}]);
BRANCH TL_{1F} (NODE [TL_{2S};TL_{2F}])]);
BRANCH G_F (NODE [BRANCH TL_{1S} (NODE [TL_{2S};TL_{2F}]);
BRANCH TL_{1F} (NODE [TL_{2S};TL_{2F}])])]$\big)$

3.1.2 Formal ET Reduction and Partitioning

The second step of the ET analysis, *Step 2 (Reduction)*, is used to reduced its number of ET test cases. Therefore, in HOL4 we define a reduction function ⊠ that takes a list of ET paths L, which is the output of $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$, a list of ET path numbers N to be reduced and their K conditional events CE and returns a reduced ET model as:

Definition 3.6. *Complete ET Model Reduction*

$\vdash$ L ⊠ N CE p =

LUPDATE (ET_{PATH} p CE) (LAST N) (DELETE_N L (TAKE (LENGTH N-1) N))

To ensure the correctness of the reduced ET model, we formally verify that the length of the new ET model after reduction is equal to the length of generated complete ET model $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ minus the number of paths that were deleted, in HOL4 as:

Theorem 3.2. *Verification of the Reduced ET Model Length*

$\vdash$ INDEX_LT_LEN N (L $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ $\mathrm{L}_{\mathcal{N}}$) $\wedge$ LENGTH N $\geq$ 1 $\Rightarrow$

LENGTH $\big($(L $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ $\mathrm{L}_{\mathcal{N}}$) ⊠ N CE p$\big)$ = LENGTH (L $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ $\mathrm{L}_{\mathcal{N}}$) $-$ LENGTH N $+$ 1

where INDEX_LT_LEN ensures that the length N is less than the length of the ET list. Upon this, the reduced ET model corresponding to the actual behavior of the Micro-Grid system through reducing the ET paths 4-7 with respect to the failure of the generator (G_F), as shown in Figure 2.2(b), can be obtained in HOL4 as:

Definition 3.7. *Micro-Grid Reduced ET Model*

$$\vdash \texttt{MicroGrid\_Reduced\_ET [}\mathrm{G};\mathrm{TL}_1;\mathrm{TL}_2\texttt{] [4-7] [}\mathrm{G}\downarrow\texttt{] =}$$

$$\texttt{ETREE}\ \big(\texttt{NODE}\ \big(\texttt{(}{\uparrow\downarrow}\ \texttt{[}\mathrm{G};\mathrm{TL}_1\texttt{]}\ \bigotimes_{\mathrm{L}}^{\mathcal{N}}\ {\uparrow\downarrow}\ \texttt{[}\mathrm{TL}_2\texttt{])}\ \boxtimes\ \texttt{[4-7] [}\mathrm{G}\downarrow\texttt{]}\big)\big)$$

where the function $\uparrow\downarrow$ takes an arbitrary list of $\mathcal{N}$ components and assigns failure and reliability states $\downarrow$ and $\uparrow$ to each component, respectively (see Section 2.4). We can formally verify the above Micro-Grid reduced ET model (Figure 2.2(b)) in HOL4 as:

Theorem 3.3. *Verification of the Micro-Grid Reduced ET Model*

$$\vdash \texttt{MicroGrid\_Reduced\_ET [}\mathrm{G};\mathrm{TL}_1;\mathrm{TL}_2\texttt{] [4-7] [}\mathrm{G}\downarrow\texttt{] =}$$

$$\begin{aligned}\texttt{ETREE}\ \big(\texttt{NODE [BRANCH }\mathrm{G}\uparrow\texttt{ (NODE [BRANCH }\mathrm{TL}_1\uparrow\texttt{ (NODE [}\mathrm{TL}_2\uparrow\texttt{; }\mathrm{TL}_2\downarrow\texttt{]);}\\ \texttt{BRANCH }\mathrm{TL}_1\downarrow\texttt{ (NODE [}\mathrm{TL}_2\uparrow\texttt{; }\mathrm{TL}_2\downarrow\texttt{])]);}\\ \mathrm{G}\downarrow\texttt{]}\big)\end{aligned}$$

To perform multiple reduction operations on a given ET model, we define a reduction function $\boxtimes^{\mathcal{N}}$ that recursively applies $\boxtimes$ on a given two-dimensional list, in HOL4 as:

Definition 3.8. *Multiple ET model Reductions*

$$\vdash \texttt{L}\ \boxtimes^{\mathcal{N}}\ \texttt{(N::Ns) (CE::CEs) p = (L}\ \boxtimes\ \texttt{N CE p)}\ \boxtimes^{\mathcal{N}}\ \texttt{Ns CEs p}$$

where `L` is the list of a generated complete ET model (the output of Definition 3.4), `N` is the list of the first ET paths to be reduced, `Ns` is the list of all the remaining ET paths to be reduced, `CE` is the list of the first conditional events, `CEs` is the list of all the remaining given conditional events and `p` is the probability space.

After the ET reduction process, the next step of ET analysis, *Step 3 (Partitioning)*, we define a partitioning function $\boxplus$ to extract a collection of ET paths specified in the index list `N` from the reduced ET model list `L`, in HOL4 as follows:

Definition 3.9. *ET Paths Partitioning*

$$\vdash \texttt{N}\ \boxplus\ \texttt{L = MAP (}\lambda\texttt{a. EL a L) N}$$

For instance, the complete failure paths of the Micro-Grid system, i.e., paths 3 and 4, as shown in Figure 2.2(b), can be extracted in HOL4 as:

Definition 3.10. *Micro-Grid Complete Failure*

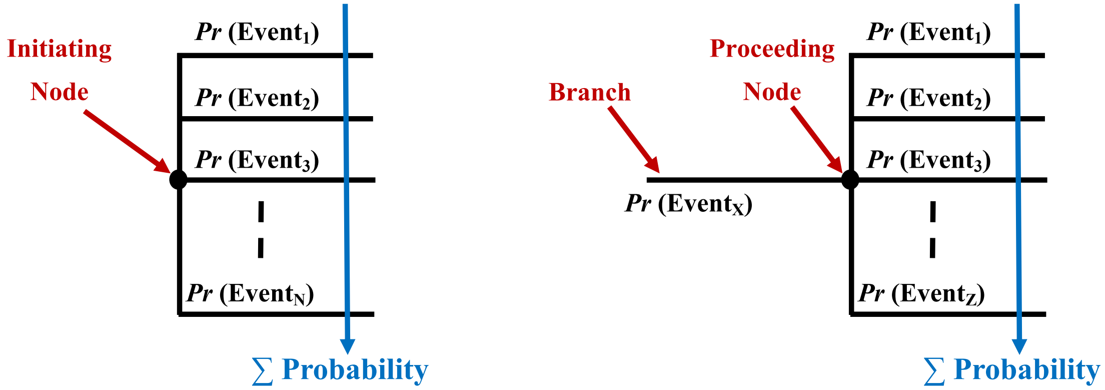
$\vdash$ `MicroGrid_Complete_Failure [3;4]` [G;TL$_1$;TL$_2$] `[4-7]` [G $\downarrow$] `=`

`ETREE` $\big($`NODE ([3;4]` $\boxplus$ `MicroGrid_Reduced_ET` [G;TL$_1$;TL$_2$] `[4-7]` [G $\downarrow$]`))`$\big)$

3.1.3 Formal ET Probabilistic Analysis

For the formal ET probabilistic analysis, we verified in HOL4 the mathematical ET probabilistic formulations for `NODE`, `BRANCH` and ET$_{PATH}$ [13]. These formulations can be used to easily evaluate the probabilities of all possible scenarios of large-scale ET models that consist of $\mathcal{N}$ components and each component consists of $\mathcal{M}$-states.

Formula 1: The probability of $\mathcal{N}$ failure/reliability events (from Event$_1$ to Event$_\mathcal{N}$) constructed in an ET initiating node, as shown in Figure 3.3(a), is verified as the sum of probabilities associated with the events (i.e., Pr(Event$_1$) + Pr(Event$_2$) + Pr(Event$_3$) +...+ Pr(Event$_{\mathcal{N}-1}$) + Pr(Event$_\mathcal{N}$)).



(a) ET Node

(b) ET Branch

Figure 3.3: Probability of ET Basic Constructors

Theorem 3.4. *Probability of ET Node Events*

$\vdash$ $\texttt{prob\_space p} \wedge (\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{N}) \in \texttt{events p} \wedge \Omega_C^\mathcal{N}\ (\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{N})$

$\quad\Rightarrow \texttt{prob p}\ \big(\texttt{ETREE (NODE (}\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{N}\texttt{))}\big) \texttt{ = } \sum\ \big(\mathrm{Pr_L}\ \texttt{p}\ (\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{N})\big)$

where the functions $\sum$ and $\mathrm{Pr_L}$ are described in Table 2.2. The constraint `prob_space p` ensures that *p* is a valid probability space while `events p` ensures that all events in a node belong to the events space *p*. The constraint $\Omega_C^\mathcal{N}$ is defined in HOL4 to ensure that all multi-state events of system components in the given list are *disjoint* (cannot occur at the same time) and *distinct* (not similar to each other), as:

Definition 3.11. *ET Component Constraints*

$\vdash \Omega_C^\mathcal{N}\ (\mathcal{C}_1\texttt{::}\mathcal{C}_\mathcal{N}) \Leftrightarrow \texttt{ALL\_DISTINCT}\ \mathcal{C}_1 \wedge \texttt{disjoint}\ \mathcal{C}_1 \wedge \Omega_C^\mathcal{N}\ \mathcal{C}_\mathcal{N}$

Formula 2: The probability of a specific failure/reliability event Event_X in an ET branch connected to a proceeding node of Z events (from Event_1 to $\mathrm{Event}_\mathcal{Z}$), as shown in Figure 3.3(b), is equal to the sum of multiplication of the branch event probability with each of the probabilities for the next node events, i.e., $Pr(\mathrm{Event}_X) \times Pr(\mathrm{Event}_1) + Pr(\mathrm{Event}_X) \times Pr(\mathrm{Event}_2) + \ldots + Pr(\mathrm{Event}_X) \times Pr(\mathrm{Event}_\mathcal{Z})$.

Theorem 3.5. *Probability of ET Branch Events*

$\vdash \texttt{prob\_space p} \wedge \Omega_C^\mathcal{N}\ (\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{Z}) \wedge (\mathrm{E}_X\texttt{::}\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{Z}) \in \texttt{events p} \wedge$

$\quad\texttt{MUTUAL\_INDEP p}\ (\mathrm{E}_X\texttt{::}\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{Z})$

$\quad\Rightarrow \texttt{prob p}\ \big(\texttt{ETREE (BRANCH}\ \mathrm{E}_X\ \texttt{(NODE (}\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{Z}\texttt{)))}\big) \texttt{ =}$

$\qquad\qquad(\texttt{prob p}\ \mathrm{E}_X) \times \sum\ \big(\mathrm{Pr_L}\ \texttt{p}\ (\mathrm{E}_1\texttt{::}\mathrm{E}_\mathcal{Z})\big)$

where `MUTUAL_INDEP` ensures that all failure and reliability events are mutually independent (see Definition 2.4).

Formula 3: The probability of an ET path consisting of cascading $\mathcal{M}$ failure and success events, as shown in Figure 3.4(a), can be expressed mathematically as the multiplication of the individual probabilities of all $\mathcal{M}$ events associated with it.

Theorem 3.6. *Probability of an ET Path of $\mathcal{M}$ Events*

$\vdash$ $\texttt{prob\_space p} \land \texttt{MUTUAL\_INDEP p } (\mathrm{E}_1\texttt{::}\mathrm{E}_{\mathcal{M}}) \land (\mathrm{E}_1\texttt{::}\mathrm{E}_{\mathcal{M}}) \in \texttt{events p}$

$\Rightarrow \texttt{prob p } \big(\mathrm{ET}_{PATH}\texttt{ p } (\mathrm{E}_1\texttt{::}\mathrm{E}_{\mathcal{M}})\big) \texttt{ = } \prod \big(\mathrm{Pr}_{\mathrm{L}}\texttt{ p } (\mathrm{E}_1\texttt{::}\mathrm{E}_{\mathcal{M}})\big)$

where the function $\prod$ returns the product of the list elements.

Formula 4: A complex two-dimensional generic ET probabilistic formulation for extracting a collection of $\mathcal{N}$ paths and each path is associated with different $\mathcal{M}$ events from an ET model, as shown in Figure 3.4(b), can be expressed mathematically as the sum of the recursive multiplication of individual probabilities for all its ET paths.

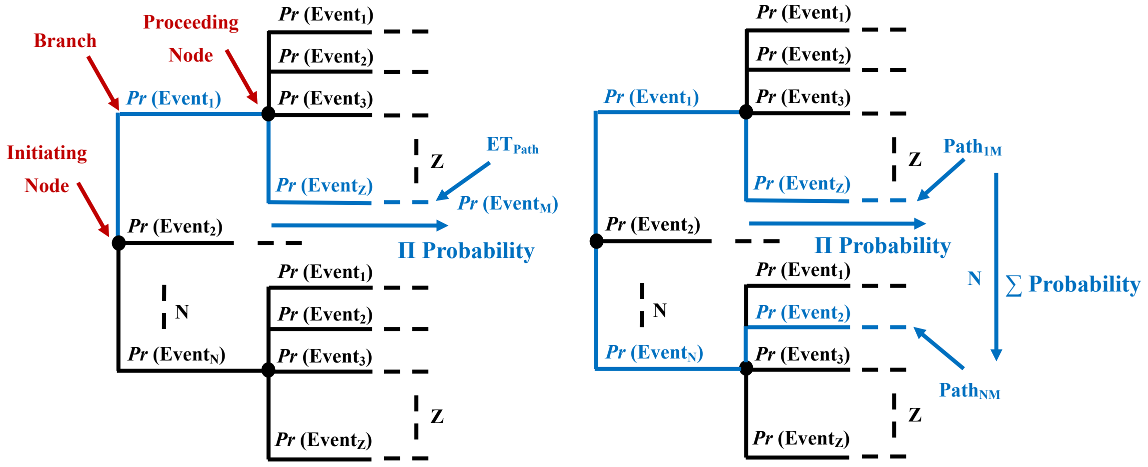
Theorem 3.7. *Probability of Complex $\mathcal{N}$ ET Paths of $\mathcal{M}$ Events*

$\vdash$ $\texttt{prob\_space p} \land \texttt{MUTUAL\_INDEP p } (\mathrm{Path}_{1_{\mathcal{M}}}\texttt{::}\mathrm{Path}_{\mathcal{N}_{\mathcal{M}}}) \land$

$(\mathrm{Path}_{1_{\mathcal{M}}}\texttt{::}\mathrm{Path}_{\mathcal{N}_{\mathcal{M}}}) \in \texttt{events p}$

$\Rightarrow \texttt{prob p } \big(\texttt{ETREE } \big(\texttt{NODE } (\texttt{MAP } (\lambda\texttt{a. } \mathrm{ET}_{PATH}\texttt{ p a}) \; (\mathrm{Path}_{1_{\mathcal{M}}}\texttt{::}\mathrm{Path}_{\mathcal{N}_{\mathcal{M}}}))\big)\big)$

$\texttt{ = } \sum \big(\texttt{MAP } (\lambda\texttt{a. } \prod \; (\mathrm{Pr}_{\mathrm{L}}\texttt{ p a})) \; (\mathrm{Path}_{1_{\mathcal{M}}}\texttt{::}\mathrm{Path}_{\mathcal{N}_{\mathcal{M}}})\big)$



(a) An ET Path of $\mathcal{M}$ Events

(b) $\mathcal{N}$ ET Paths of $\mathcal{M}$ Events

Figure 3.4: Probability of Generic ET Paths

3.2 Formal ET Analysis Process

Based on the ET formalizations provided in the previous sections, Figure 3.5 describes the steps to formally analyze a given safety-critical system. At the beginning, the reliability engineer provides the safety-critical system diagram and its description. The first step is to generate a complete complex ET model (Step 1) using our formalization of ET modeling structure in HOL4. The second step is to reduce the number of possible test cases (Step 2) using our ET reduction functions in HOL4. The next step is to partition the ET model based on the reliability requirements (Step 3) according to the reliability requirements of the given system. The last step is to perform the probabilistic analysis of the occurrence of certain events (Step 4) using our formally verified probabilistic theorems and the given failure distributions to all system components. Based on the formally verified expressions of reliability, several reliability indices can be evaluated for critical decision making, as it will be described in the next section.

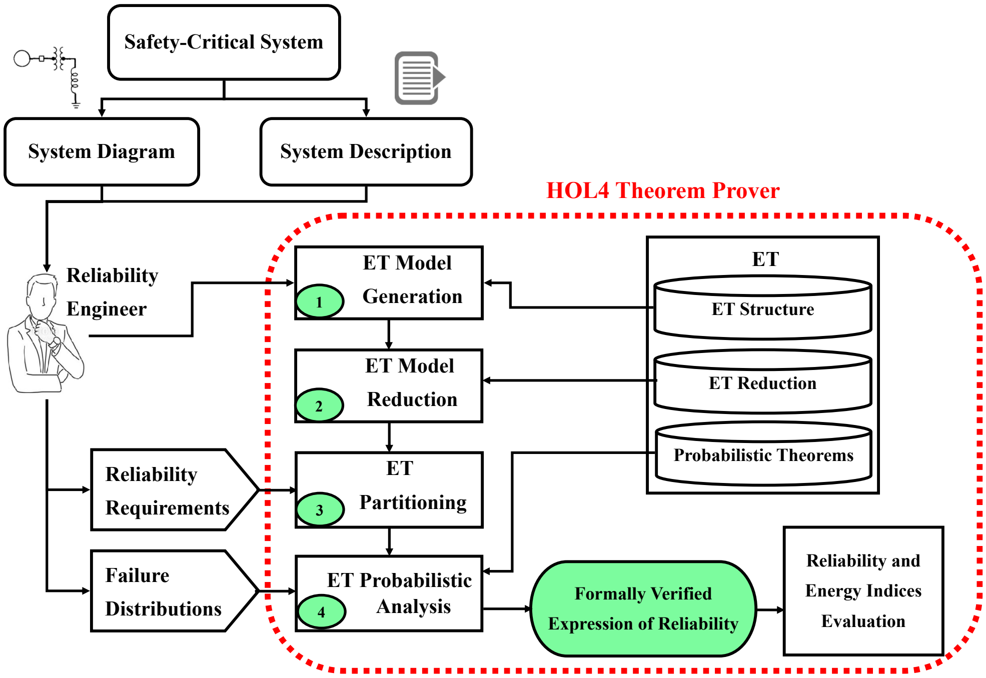


Figure 3.5: Methodology for Formal Probabilistic ET Analysis

3.3 Applications: Electrical Power Systems

To illustrate the applicability of our proposed approach, we define several ET reliability indices in HOL4, then we present the formal ET reliability analysis of several power systems: (1) a *two-state* ET model of the standard IEEE 3-Bus bulk power system; (2) a *multi-state* ET model of HVDC coupling between Québec and New England; and (3) a *two-state* multiple ET models of IEEE 118-bus power network.

3.3.1 Formal ET Reliability and Energy Indices

During the design stage, planners need to evaluate some significant reliability indices [65], which are based on ET analysis and they are formalized as following.

ET Reliability Indices

SAIFI is defined as the total number of customer interruptions (power outage ↯) over the total number of customers served. SAIDI is defined as the sum of all customer interruption durations over the total number of customers served while CAIDI is defined as the sum of all customer interruption durations over the total number of customer interruptions. ASAI is defined as the customer hours of available service over the customer hours demanded while ASUI is defined as the complement of ASAI [65].

$$\mathrm{SAIFI} = \frac{\text{Total Number of Customer Interruptions}}{\text{Total Number of Customers Served}} = \frac{\sum_{Pr(X_{\lightning})\times \mathrm{CN}_X}}{\sum_{\mathrm{CN}_X}} \tag{3.1}$$

$$\mathrm{SAIDI} = \frac{\text{Total Number of Customer Interruption Durations}}{\text{Total Number of Customers Served}} = \frac{\sum_{Pr(X_{\lightning})\times \mathrm{MTTR}_X \times \mathrm{CN}_X}}{\sum_{\mathrm{CN}_X}} \tag{3.2}$$

$$\mathrm{CAIDI} = \frac{\text{Total Number of Customer Interruption Durations}}{\text{Total Number of Customer Interruptions}} = \frac{\mathrm{SAIDI}}{\mathrm{SAIFI}} \tag{3.3}$$

$$\mathrm{ASAI} = \frac{\text{Customer Hours of Available Service}}{\text{Customer Hours Demanded}} = \frac{\sum_{\mathrm{CN}_X \times 8760} - \sum_{Pr(X_{\lightning}) \times \mathrm{MTTR}_X \times \mathrm{CN}_X}}{\sum_{\mathrm{CN}_X \times 8760}} \tag{3.4}$$

$$\mathrm{ASUI} = 1 - \mathrm{ASAI} = \frac{\text{Customer Hours of Unavailable Service}}{\text{Customer Hours Demanded}} = \frac{\sum_{Pr(X_{\lightning}) \times \mathrm{MTTR}_X \times \mathrm{CN}_X}}{\sum_{\mathrm{CN}_X \times 8760}} \tag{3.5}$$

where CN_X is the total number of customers served in the smart power grid at a specific location X for which the reliability indices are calculated while MTTR_X is the mean-time-to-repair the failure that occurred at the location X. We formally define a function `SAIFI` in HOL4 in three parts corresponding to Equation 3.1 as follows:

Definition 3.12. *Probability of Location X Complete/Partial Failure*

$$\vdash \texttt{Prob}^{\texttt{ET}}_{\texttt{X}}\lightning\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}\ \texttt{p} =$$
$$\texttt{prob p}\ \Big(\texttt{ETREE}\ \big(\texttt{NODE}\ (\texttt{E} \boxplus (\texttt{L} \bigotimes^{\mathcal{N}}_{\mathrm{L}} \texttt{L}_{\mathcal{N}}) \boxtimes^{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}})\big)\Big)$$

where `L`, $\texttt{N}_{\mathcal{N}}$, $\texttt{CE}_{\mathcal{N}}$, `E` are list of all components modes, last component modes, list of all CCs, list of all CEs, list of partitioning paths for power outage $\lightning$, respectively.

Definition 3.13. *Total Number of Load Customer Interruptions*

$$\vdash \textstyle\sum^{\texttt{Interrupt}}_{\texttt{Load}}\lightning\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ (\texttt{E::E}_{\mathcal{N}})\ (\texttt{CN::CN}_{\mathcal{N}})\ \texttt{p} =$$
$$\Big(\texttt{Prob}^{\texttt{ET}}_{\texttt{X}}\lightning\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}\ \texttt{p}\Big) \times \texttt{CN} + \textstyle\sum^{\texttt{Interrupt}}_{\texttt{Load}}\lightning\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}$$

where $\texttt{E}_{\mathcal{N}}$ is a list of all partitioning paths for complete/partial failure events while $\texttt{CN}_{\mathcal{N}}$ is a list of all load customer numbers affected by the failures occurrence.

Definition 3.14. *SAIFI Reliability Index*

$$\vdash \texttt{SAIFI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} = \frac{\sum^{\texttt{Interrupt}}_{\texttt{Load}}\lightning\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \mathrm{p}}{\sum \texttt{CN}_{\mathcal{N}}}$$

Similarly, we formally define time duration function $\sum^{\texttt{Duration}}_{\texttt{Load}}\lightning$ and generic function `SAIDI`, as described in Equation 3.2, respectively, in HOL4 as:

Definition 3.15. *Total Number of Load Customer Interruption Durations*

$$\vdash \sum\nolimits_{\texttt{Load}}^{\texttt{Duration}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ (\texttt{E::E}_{\mathcal{N}})\ (\texttt{MTTR::MTTR}_{\mathcal{N}})\ (\texttt{CN::CN}_{\mathcal{N}})\ \texttt{p} =$$

$$\left(\texttt{Prob}_{\texttt{X}}^{\texttt{ET}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}\ \texttt{p}\right) \times \texttt{MTTR} \times \texttt{CN} +$$

$$\sum\nolimits_{\texttt{Load}}^{\texttt{Duration}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}$$

where $\texttt{MTTR}_{\mathcal{N}}$ is the list of MTTRs for all customer loads.

Definition 3.16. *SAIDI Reliability Index*

$$\vdash \texttt{SAIDI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} =$$
$$\frac{\sum\nolimits_{\texttt{Load}}^{\texttt{Duration}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\sum \texttt{CN}_{\mathcal{N}}}$$

Using Definitions 3.14-3.16, we formally define *generic* functions for `CAIDI`, `ASAI`, `ASUI` corresponding to Equations 3.3, 3.4 and 3.5, respectively, in HOL4 as:

Definition 3.17. *CAIDI Reliability Index*

$$\vdash \texttt{CAIDI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} =$$
$$\frac{\texttt{SAIDI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\texttt{SAIFI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}$$

Definition 3.18. *ASAI Reliability Index*

$$\vdash \texttt{ASAI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} =$$
$$\frac{\sum \texttt{CN}_{\mathcal{N}} \times 8760 - \sum\nolimits_{\texttt{Load}}^{\texttt{Duration}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\sum \texttt{CN}_{\mathcal{N}} \times 8760}$$

Definition 3.19. *ASUI Reliability Index*

$$\vdash \texttt{ASUI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} =$$

$$\texttt{1 - ASAI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} =$$
$$\frac{\sum\nolimits_{\texttt{Load}}^{\texttt{Duration}} \lightning \ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\sum \texttt{CN}_{\mathcal{N}} \times 8760}$$

ET Energy Indices

Energy Not Supplied Index (ENS) is defined as the total energy not supplied by the utility. Average System Curtailment Index (ASCI) is defined as the the total energy not supplied over total number of customer served. Loss of Load Expectation (LOLE) is defined as the sum of all probabilities for losing certain loads on a specific day, which are obtained from the Capacity Outage Probability Table (COPT) using ET analysis. LOLE is defined as the sum of expected number of days in a specific period the daily load will exceed the available capacity. The per unit Loss of Energy Expectation (LOEE) value represents the ratio between the energy curtailed by a possible capacity outage and the total load energy required to serve the system demand. Energy Index of Reliability (EIR) is defined as the complement of the per unit LOEE.

$$\mathrm{ENS} = \text{Total Energy Not Supplied by the System} = \sum_{X=1}^{\mathcal{N}} \mathrm{L}_{a(X)} \times Pr(X_{\lightning}) \times \mathrm{MTTR}_X \tag{3.6}$$

where $\mathrm{L}_{a(X)}$ is the average load connected to a load of location X.

$$\mathrm{ASCI} = \frac{\text{Total Energy Not Supplied}}{\text{Total Number of Customers Served}} = \frac{\sum_{X=1}^{\mathcal{N}} \mathrm{L}_{a(X)} \times Pr(X_{\lightning}) \times \mathrm{MTTR}_X}{\sum_{\mathrm{CN}_X}} \tag{3.7}$$

$$\mathrm{LOLE} = \sum_{k=1}^{\mathcal{N}} P_k \; t_k \tag{3.8}$$

where P_k is the probability of the k^{th} possible capacity outage while t_k is the number of days/period of k^{th} outage causes load loss.

$$\mathrm{LOEE}_{\mathrm{p.u.}} = \frac{\sum_{k=1}^{\mathcal{N}} E_k \; P_k}{\mathrm{E}_T} \tag{3.9}$$

where E_k is the energy curtailed by the capacity outage while E_T is the total energy required by consumers.

$$\mathrm{EIR} = 1 - \mathrm{LOEE}_{\mathrm{p.u.}} \tag{3.10}$$

We can define functions corresponding to Equations 3.6-3.10 by utilizing the function $\texttt{Prob}_X^{ET}\text{↯}$, respectively, as follows:

Definition 3.20. *ENS Energy Index*

$$\begin{aligned}
&\vdash \texttt{ENS (La::La}_{\mathcal{N}}\texttt{) L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ (E::E}_{\mathcal{N}}\texttt{) (MTTR::MTTR}_{\mathcal{N}}\texttt{) p =}\\
&\quad \texttt{La} \times \left(\texttt{Prob}_{\texttt{X}}^{\texttt{ET}}\text{↯}\ \texttt{L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E p}\right) \times \texttt{MTTR +}\\
&\quad \texttt{ENS La}_{\mathcal{N}}\texttt{ L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ MTTR}_{\mathcal{N}}\texttt{ p}
\end{aligned}$$

where $\texttt{La}_{\mathcal{N}}$ is the list of load demands connected at all locations in the power system.

Definition 3.21. *ASCI Energy Index*

$$\begin{aligned}
&\vdash \texttt{ASCI La}_{\mathcal{N}}\texttt{ L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ MTTR}_{\mathcal{N}}\texttt{ CN}_{\mathcal{N}}\texttt{ p =}\\
&\quad \frac{\texttt{ENS La}_{\mathcal{N}}\texttt{ L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ MTTR}_{\mathcal{N}}\texttt{ p}}{\sum \texttt{CN}_{\mathcal{N}}}
\end{aligned}$$

Definition 3.22. *LOLE Energy Index*

$$\begin{aligned}
&\vdash \texttt{LOLE L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ (E::E}_{\mathcal{N}}\texttt{) (tk::tk}_{\mathcal{N}}\texttt{) p =}\\
&\quad \left(\texttt{Prob}_{\texttt{X}}^{\texttt{ET}}\text{↯}\ \texttt{L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E p}\right) \times \texttt{tk + LOLE L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ tk}_{\mathcal{N}}\texttt{ p}
\end{aligned}$$

where $\texttt{tk}_{\mathcal{N}}$ is the list of number of days curtailed by all possible outages.

Definition 3.23. *LOEE Energy Index*

$$\begin{aligned}
&\vdash \texttt{LOEE L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ (E::E}_{\mathcal{N}}\texttt{) CE}_{\mathcal{N}}\texttt{ (Ek::Ek}_{\mathcal{N}}\texttt{) p =}\\
&\quad \left(\texttt{Prob}_{\texttt{X}}^{\texttt{ET}}\text{↯}\ \texttt{L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E p}\right) \times \texttt{Ek + LOEE L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ Ek}_{\mathcal{N}}\texttt{ p}
\end{aligned}$$

where $\texttt{Ek}_{\mathcal{N}}$ is the list of all energy curtailed by the outages.

Definition 3.24. *EIR Energy Index*

$$\begin{aligned}
&\vdash \texttt{EIR L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ Ek}_{\mathcal{N}}\texttt{ EN}_{\mathcal{N}}\texttt{ E}_{T}\texttt{ p =}\\
&\quad \texttt{1 - }\frac{\texttt{LOEE L L}_{\mathcal{N}}\texttt{ N}_{\mathcal{N}}\texttt{ CE}_{\mathcal{N}}\texttt{ E}_{\mathcal{N}}\texttt{ Ek}_{\mathcal{N}}\texttt{ p}}{\texttt{E}_{T}}
\end{aligned}$$

3.3.2 IEEE 3-Bus Composite Bulk Power System

For power grids reliability assessment, power engineers have been dividing the grid into three main Hierarchical Levels (HL) [66]: (a) HL-I: generation systems and their ability to satisfy the pooled system demand; (b) HL-II: composite generation and transmission (or bulk power) systems and their ability to deliver energy to the bulk supply points; and (c) HL-III: complete grid system including distribution and its ability to satisfy the capacity and energy demands of individual consumers. We can use our methodology in Section 3.2 for the formal probabilistic risk assessment of any hierarchical level. In this case study, we focus on the composite generation and transmission systems, i.e., hierarchical level II. Consider a standard IEEE 3-bus power grid system [67] consisting of three main transmission lines (M), two lateral transmission lines (L), two Generators (G), three substations and three different loads A, B and C with the number of customers served CN_A, CN_B and CN_C, respectively, as shown in Figure 3.6.

Formal Two-State ET Model

Step 1 (ET Generation):

We assume that each generator (G1, G2), each transmission line (M1, M2, M3, L1, L2) is represented by only two state model (Figure 3.1), i.e., Failure (F) or Success (S). Using $\bigotimes_{\text{L}}^{\mathcal{N}}$ we can generate the complete ET model of the whole electrical bulk power grid system with a total possible scenario of 128 test cases, in HOL4 as follows:

Definition 3.25. *IEEE 3-Bus Complete ET Model (128 Test Cases)*

$\vdash$ `Bulk_Power_Grid_Complete_ET [G1;G2;M1;M2;M3;L1;L2] =`

`ETREE (NODE (`$\uparrow\downarrow$` [G1;G2;M1;M2;M3;L1]) `$\bigotimes_{\text{L}}^{\mathcal{N}}$` (`$\uparrow\downarrow$` [L2]))`

where the function $\uparrow\downarrow$ takes a list of $\mathcal{N}$ components and assigns failure $\downarrow$ and reliability $\uparrow$ distributions (see Section 2.4) to each component.

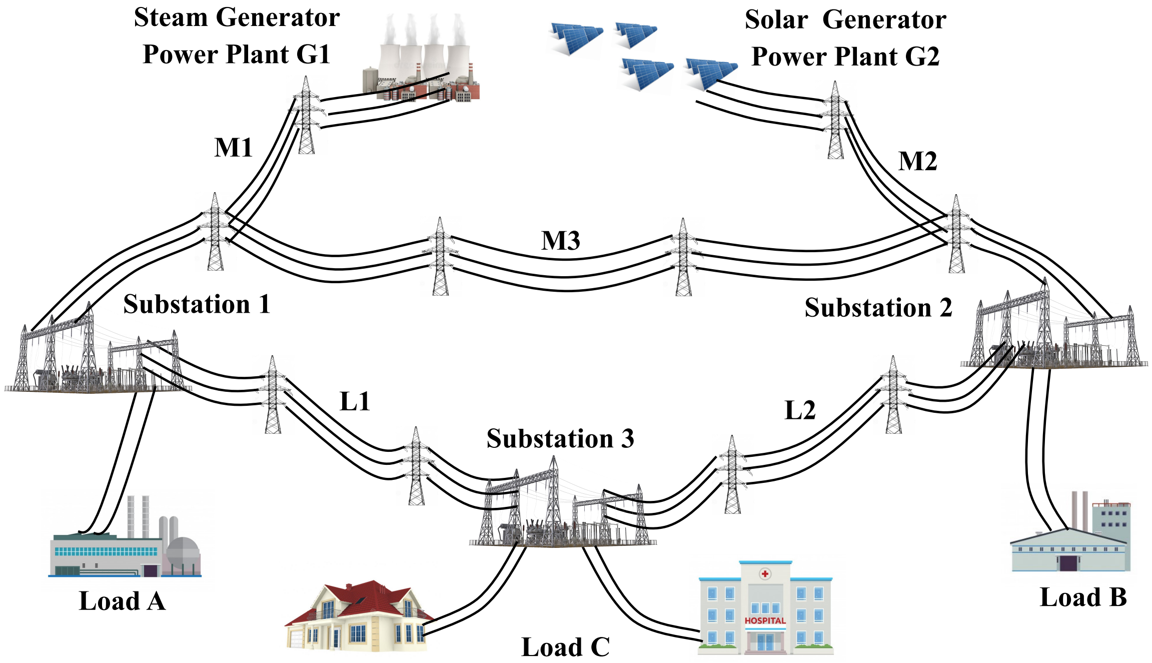


Figure 3.6: IEEE 3-Bus Electrical Power Grid System

Step 2 (ET Reduction):

The generated complete ET of the bulk power grid, obtained above, can be reduced from 128 paths (0-127) to 27 paths (0-26). Using the *generic* reduction function $\boxtimes^{\mathcal{N}}$ (see Section 3.1.2), we can formally describe the reduced ET model of the electrical power grid, as shown in Figure 3.7, in HOL4 as:

Definition 3.26. *IEEE 3-Bus Reduced ET Model (27 Test Cases)*

⊢ Bulk_Power_Grid_Reduced_ET

    [G1;G2;M1;M2;M3;L1;L2] [[96-127];[80-95];...]

    [[G1 ↓;G2 ↓];[G1 ↓;G2 ↑;M1 ↓];...] =

ETREE (NODE (↑↓ [G1;G2;M1;M2;M3;L1]) $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ (↑↓ [L2])

  $\boxtimes^{\mathcal{N}}$ [[96-127];[80-95];...] [[G1 ↓;G2 ↓];[G1 ↓;G2 ↑;M1 ↓];...])

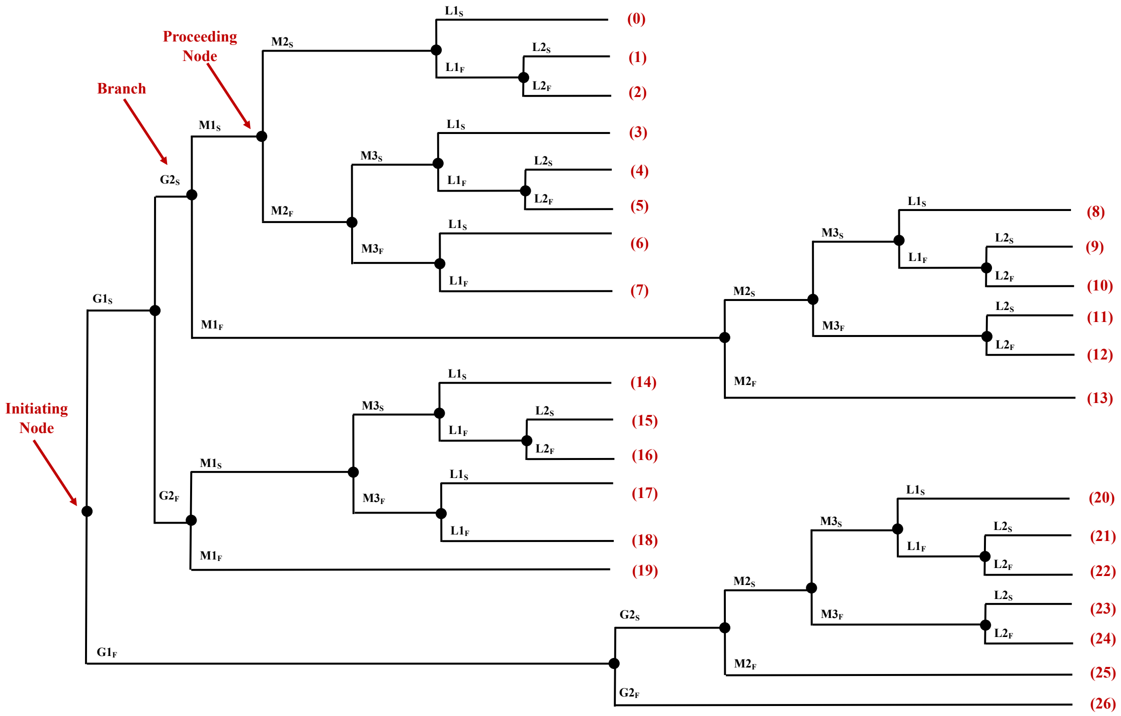


Figure 3.7: Reduced ET of the Electrical Power Grid

Step 3 (ET Partitioning):

Typically, we are only interested in the occurrence of certain consequence failure/reliability events in the ET diagram. For instance, if we consider the complete failure ↯ of load A, then ET paths 11-13, 19, 23-25 and 26 are obtained. Similarly, a different collection of the ET paths can be obtained by observing different grid failures as:

1. $Pr(\text{Load}_A ↯) = \sum Pr(ET_{paths}\ 11-13,\ 19,\ 23-25,\ 26)$

2. $Pr(\text{Load}_B ↯) = \sum Pr(ET_{paths}\ 6,\ 7,\ 13,\ 17-19,\ 25,\ 26)$

3. $Pr(\text{Load}_C ↯) = \sum Pr(ET_{paths}\ 2,\ 5,\ 7,\ 10,\ 12,\ 13,\ 22,\ 24-26)$

Using our ET partitioning function ⊞ (see Section 3.1.2), we can select different ET paths from the generated reduced ET model of the power network, in HOL4 as follows:

Definition 3.27. *IEEE 3-Bus Load A Failure*

```
⊢ Bulk_Power_Grid_Load_A_Failure
        [G1;G2;M1;M2;M3;L1;L2] [[96-127];[80-95];...]
        [[G1 ↓;G2 ↓];[G1 ↓;G2 ↑;M1 ↓];...]  [11-13; 19; 23-25; 26] =
  ETREE
   (NODE
     [11-13; 19; 23-25; 26] ⊞
     (↑↓ [G1;G2;M1;M2;M3;L1]) ⨂^𝒩_L (↑↓ [L2])
     ⊠^𝒩 [[96-127];[80-95];...]  [[G1 ↓;G2 ↓];[G1 ↓;G2 ↑;M1 ↓];...])
```

Similarly, we can define the complete failure consequence ET scenarios `Bulk_Power_Grid_Load_B_Failure` and `Bulk_Power_Grid_Load_C_Failure` corresponding to Load B and C failures in the bulk power grid, respectively.

Formal ET Reliability Indices Assessment

The assessment of the SAIFI and SAIDI for the Electrical Power Network (EPN) shown in Figure 3.6 using Equations 3.1 and 3.2 can be written mathematically, as:

$$SAIFI_{EPN} = \frac{Pr(\text{Load}_A\text{↯}) \times \text{CN}_A + Pr(\text{Load}_B\text{↯}) \times \text{CN}_B + Pr(\text{Load}_C\text{↯}) \times \text{CN}_C}{\text{CN}_A + \text{CN}_B + \text{CN}_C} \tag{3.11}$$

$$SAIFI_{EPN} = \frac{\begin{array}{c} Pr(\text{Load}_A\text{↯}) \times \text{CN}_A \times \text{MTTR}_A + Pr(\text{Load}_B\text{↯}) \times \text{CN}_B \times \text{MTTR}_B + \\ Pr(\text{Load}_C\text{↯}) \times \text{CN}_C \times \text{MTTR}_C \end{array}}{\text{CN}_A + \text{CN}_B + \text{CN}_C} \tag{3.12}$$

Using the SAIFI formulation in Definition 3.14 with the assumption of continuous exponential distribution, we can generate the above mathematical expression of $SAIFI_{EPN}$, in HOL4 as:

Theorem 3.8. *Verification of SAIFI for the IEEE 3-Bus Bulk Power Grid*

$\vdash$ `SAIFI =`

$$\frac{\begin{array}{l}\Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times \mathrm{e}^{(-\lambda_{L2}t)} + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) + \cdots + \ldots\Big) \times \mathrm{CN\_A} + \\ \Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times \mathrm{e}^{(-\lambda_{L1}t)} + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L1}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) + \cdots + \ldots\Big) \times \mathrm{CN\_B} + \\ \Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{L1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times \cdots \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \cdots + \ldots\Big) \times \mathrm{CN\_C}\end{array}}{(\mathrm{CN\_A} + \mathrm{CN\_B} + \mathrm{CN\_C})}$$

Similarly, we can use Equation 3.2 and Definition 3.16 to verify the mathematical expression of $SAIDI_{EPN}$, in HOL4 as:

Theorem 3.9. *Verification of SAIDI for the IEEE 3-Bus Bulk Power Grid*

$\vdash$ `SAIDI =`

$$\frac{\begin{array}{l}\Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times \mathrm{e}^{(-\lambda_{L2}t)} + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) + \ldots\Big) \times \mathrm{CN\_A} \times \mathrm{MTTR\_A} + \\ \Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times \mathrm{e}^{(-\lambda_{L1}t)} + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M3}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L1}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times (1 - \mathrm{e}^{(-\lambda_{M1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{M2}t)}) + \ldots\Big) \times \mathrm{CN\_B} \times \mathrm{MTTR\_B} + \\ \Big(\mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times \mathrm{e}^{(-\lambda_{M2}t)} \times (1 - \mathrm{e}^{(-\lambda_{L1}t)}) \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \\ \mathrm{e}^{(-\lambda_{G1}t)} \times \mathrm{e}^{(-\lambda_{G2}t)} \times \mathrm{e}^{(-\lambda_{M1}t)} \times \cdots \times (1 - \mathrm{e}^{(-\lambda_{L2}t)}) + \ldots\Big) \times \mathrm{CN\_C} \times \mathrm{MTTR\_C}\end{array}}{(\mathrm{CN\_A} + \mathrm{CN\_B} + \mathrm{CN\_C})}$$

The proof of the above-verified SAIFI and SAIDI expressions at the system level was conducted using our ET theorems in HOL4 as well as using some HOL4 tactics, such as `DEP_REWRITE_TAC`, which applies our verified theorems on the required goal, and `EVAL_TAC`, which evaluates expressions till its simplest from possible [68]. In order to validate our results, in the next subsection, we numerically evaluate the above-*verified* expressions and compare them with existing available techniques.

Numerical Results

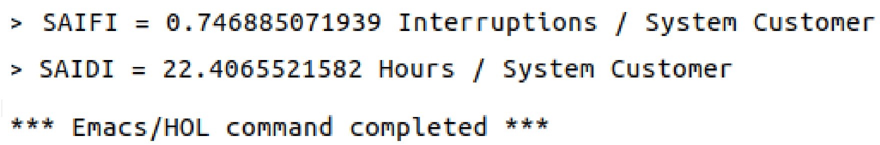
Considering the failure rates λ_{G1}, λ_{G2}, λ_{M1}, λ_{M2}, λ_{M3}, λ_{L1}, and λ_{L2} are 0.22, 0.35, 0.2, 0.5, 0.3, 0.25, 0.4 per year. Also, assuming that MTTR_A, MTTR_B, MTTR_C, are 30, 40, 25 hours/interruption [69] and CN_A, CN_B, CN_C, are 2500, 900, and 1800 customers, respectively. The reliability study is undertaken for 5 years (excluding leap years), i.e., t = (8760 (hours/year) × 5) hours. Therefore, we can evaluate SAIFI and SAIDI for the power grid (Figure 3.6) using: (1) HOL4 analysis; (2) manual mathematical analysis [13]; (3) Isograph software [18]; and (4) MATLAB MCS [70].

1. ***HOL4 Analysis***: We define SML functions [71], which can numerically evaluate the *verified* HOL4 expressions of SAIFI and SAIDI by replacing the λ symbols with the given failure rates of all subsystem components and then computing the exponential values over the time t and printing the values of the reliability indices, for example, the SML function for computing SAIFI is defined as follows:

   Definition 3.28. *SML Function for SAIFI*

   ```
   ⊢ fun SAIFI_ML X =
     val value = HOL4_EVAL X;
     print("SAIFI" ∧ "=" ∧ Real.toString (value));
     print("Interruptions / System Customer");
     end;
   ```

where the SML function `HOL4_EVAL` takes a HOL4 probabilistic expression with the failure rates and converts the string to a real value using the SML function `Real.toString`. Therefore, we can evaluate SAIFI and SAIDI for the standard IEEE 3-bus bulk power system, as shown in Figure 3.8.

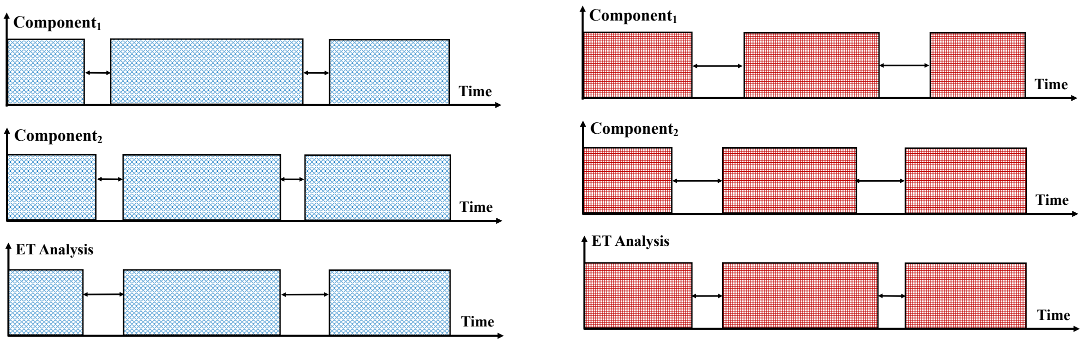


```
> SAIFI = 0.746885071939 Interruptions / System Customer
> SAIDI = 22.4065521582 Hours / System Customer

*** Emacs/HOL command completed ***
```

Figure 3.8: HOL4 Analysis: Bulk Power System SAIFI and SAIDI Results

2. *Manual Analysis*: We use a manual drawings of the ETs on a paper, then perform the manual derivations and calculations to determine the probabilities of all ET paths as well as SAIFI and SAIDI reliability indices.
3. *Isograph Software*: We use Isograph to evaluate the probabilities of all paths, then we used the manual calculation for evaluating SAIFI and SAIDI results.
4. *MATLAB Monte-Carlo Simulation*: Using random-based Monte-Carlo simulation (MCS), we can examine and predict the real functional behavior of a power grid system and estimate the average value of different reliability parameters. We use the following steps of MCS as given in [72]:
   (a) Input the expected failure rates of all components λ_G, λ_M, λ_L in *f/hours* and the expected repair times μ_G, μ_M, μ_L in hours.
   (b) Generate a random number U in the interval (0,1) for each component.
   (c) Determine the expected Time to Fail (TTF) and Time to Repair (TTR) and its consequence effect on each consumer using the ET consequence analysis method, i.e., series and parallel components, as shown in Figure 3.9(a) and Figure 3.9(b), respectively, from the equations.



(a) Two Series Components (b) Two Parallel Components

Figure 3.9: Monte-Carlo ET Analysis for Two Components

$$TTF = \frac{-\ln U}{\lambda} \qquad TTR = \frac{-\ln U}{\mu} \tag{3.13}$$

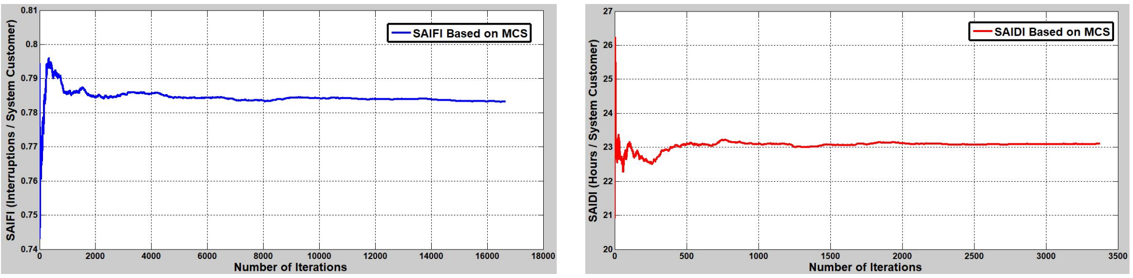
(d) Calculate the values of the reliability indices SAIFI and SAIDI for one simulated period using Equations3.1-3.2.

(e) Repeat the above iterative process for each of the simulated periods till the number of iterations exceeds 1e5 (stopping rule is reached) or the variance σ is less than 1e-5 (accepted reliability values).

(f) The average values for all the parameters are calculated and plotted.

It is evident from the above description that the MCS technique is depending on the sampling approach. Therefore, we obtain different results of SAIFI and SAIDI every run of the algorithm depending on the generated random number with a tolerance error between 4-7%. Plots of the estimates are extremely valuable and are one of the significant merits of MCS. So, Figure 3.10(a) and 3.10(b) show the best estimated results of SAIFI and SAIDI in MATLAB for the electrical bulk power system based on the MCS approach with the least errors.

A comparison of the above four methods in the assessment of the reliability indices for the power grid is presented in Table 3.1. It can be noticed that the



(a) MATLAB: SAIFI MCS Result

(b) MATLAB: SAIDI MCS Result

Figure 3.10: MATLAB MCS: Bulk Power System SAIFI and SAIDI Results

reliability indices SAIFI and SAIDI obtained from our analysis are equivalent to the corresponding ones calculated using the paper-and-pencil approach and Isograph. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results of SAIFI and SAIDI at every generation of a random number with errors in the range 4-7%. This clearly elucidates that our analysis is not only providing the correct results but also *formally proven* reliability SAIFI and SAIDI expressions (Theorems 3.8 and 3.9) compared to existing simulation tools. Moreover, the CPU time for the power grid using the HOL4 analysis is much faster than Isograph (5X) and MATLAB MCS (15X), as shown in Table 3.1. The time taken in modeling the bulk power systems using Isograph and MATLAB was almost similar while it was a bit less using the HOL4 technique and it took a much longer time for the manual analysis. The experiments were performed on a core i5, 2.20 GHz processor, Linux VM with 1 GB of RAM.

Table 3.1: Comparison of Bulk Power System SAIFI and SAIDI Results

Power Grid Reliability Indices	Manual	Isograph	MATLAB	HOL4
SAIFI (Interruptions/Customer)	0.7469	0.7469	0.7832	0.74688507194
SAIDI (Hours/Customer)	22.4066	22.4066	23.1632	22.4065521582
CPU Execution Time (Seconds)	–	8.275	25.156	1.629

3.3.3 Québec-New England HVDC Coupling

In this second case study, we endeavor to conduct formal *multi-state*-based complex ET analysis of Québec-New England HVDC Transmission system operated by Hydro-Québec power utility in Canada. Figure 3.11 [73] shows the location of Québec-New England Phase II HVDC project (2,690 MW) that have five terminals in order from North to South: Radisson, Nicolet, Des Cantons, Comerford and Sandy Pond. During normal operations, the electrical power flow [74] is passing from North (Radisson station operating as a rectifier) to South (Nicolet and Sandy Pond stations operating as inverters). We use two typical rectifier/inverter bridge system configurations [75]: (i) *Type A*: single rectifier/inverter bridge bipolar system; and (ii) *Type B*: multi rectifier/inverter bridge bipolar system, as shown in Figure 3.12 [76] and Figure 3.13 [77], respectively. *Type A* consists of 5 Transformers, 4 Bridges, 2 HVDC Lines and 4 Switches, while *Type B* consists of 10 Transformers, 8 Bridges, 2 HVDC

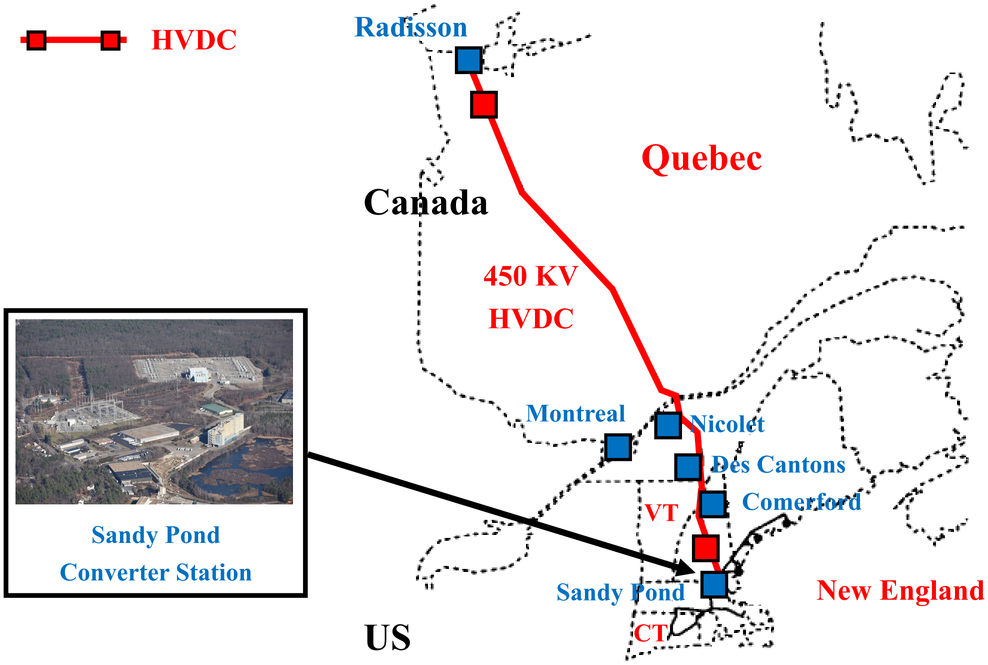


Figure 3.11: Québec-New England HVDC Coupling Between Canada and US

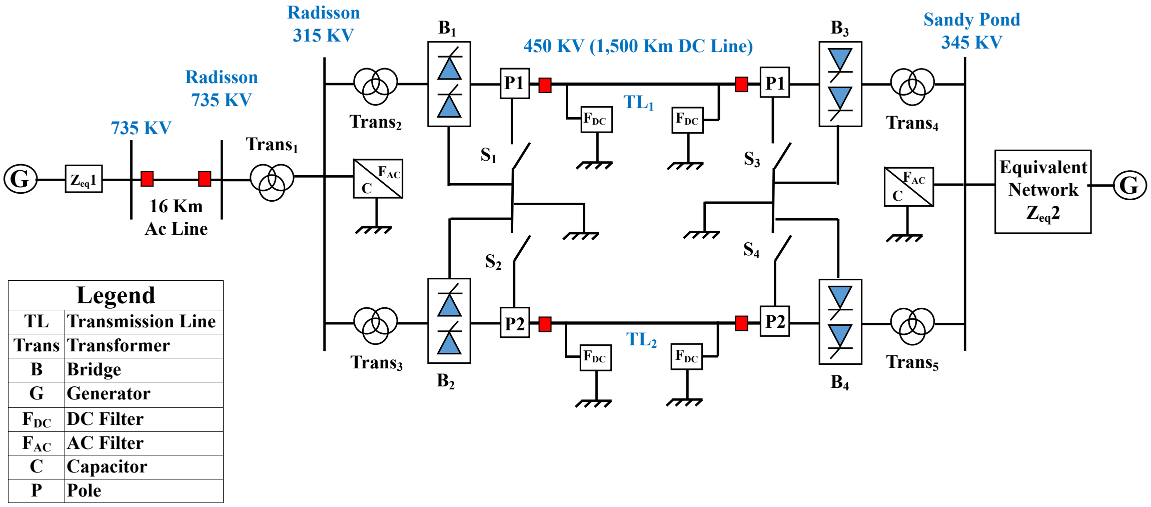


Figure 3.12: Québec-New England Single-Bridge Bipolar System

Lines and 8 Switches. We formally determine key performance energy indices COPT, ASAI, ASUI, ENS, ASCI, LOLE, LOEE, EIR, using our ET library in HOL4, which helps designers to select which HVDC type *Type A* or *Type B* is worth for implementation based on accurate, sound and fast results.

Formal Multi-State ET Model

Step 1 (ET Generation):

We assign different *multi-state* models (Fig 3.1) to each component in the HVDC transmission systems shown in Figure 3.12 and Figure 3.13, for reliability analysis as:

- Each Bridge (B) has two states, i.e., success (S) and failure (F).
- Each Transformer (TR) has three states, i.e., success, fail, and partly fail (PF).
- Each HVDC Transmission Line (TL) has 5 states, i.e., success, fail, hot reserve (HR), cold reserve (CR), fail to take up load (FTL).

Therefore, we formally describe in HOL4 the complete ET models of *Type A* and *Type B* HVDC systems ($2^4 \times 3^5 \times 5^2$ and $2^8 \times 3^{10} \times 5^2$ possible test cases, respectively), using the function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$, for instance, we generate all possible risk cases of *Type A* as:

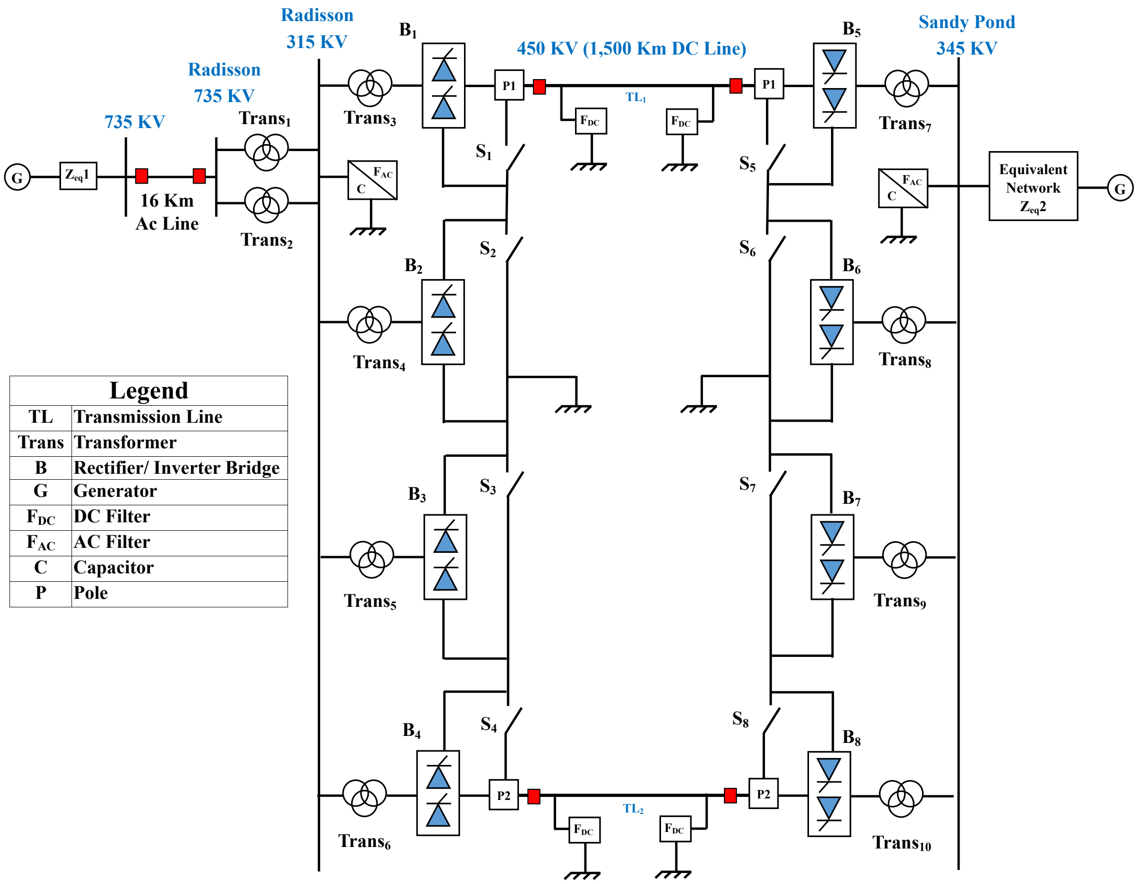


Figure 3.13: Québec-New England Multi Bridge Bipolar System

Definition 3.29. *Complete ET model of HVDC Type A*

$\vdash$ `HVDC_Type_A_Complete_ET_Model =`

`ETREE`

$\Big($`NODE`

$[[\mathrm{TR1}_S \uparrow;\mathrm{TR1}_F \downarrow;\mathrm{TR1}_{PF} \downarrow];\ [\mathrm{TR2}_S \uparrow;\mathrm{TR2}_F \downarrow;\mathrm{TR2}_{PF} \downarrow];$

$[\mathrm{TR3}_S \uparrow;\mathrm{TR3}_F \downarrow;\mathrm{TR3}_{PF} \downarrow];\ [\mathrm{B1}_S \uparrow;\mathrm{B1}_F \downarrow];\ [\mathrm{B2}_S \uparrow;\mathrm{B2}_F \downarrow];$

$[\mathrm{TL1}_S \uparrow;\mathrm{TL1}_F \downarrow;\mathrm{TL1}_{HR} \downarrow;\mathrm{TL1}_{CR} \downarrow;\mathrm{TL1}_{FTL} \downarrow];$

$[\mathrm{TL2}_S \uparrow;\mathrm{TL2}_F \downarrow;\mathrm{TL2}_{HR} \downarrow;\mathrm{TL2}_{CR} \downarrow;\mathrm{TL2}_{FTL} \downarrow];$

$[\mathrm{B3}_S \uparrow;\mathrm{B3}_F \downarrow];\ [\mathrm{B4}_S \uparrow;\mathrm{B4}_F \downarrow];\ [\mathrm{TR4}_S \uparrow;\mathrm{TR4}_F \downarrow;\mathrm{TR4}_{PF} \downarrow]]$

$\bigotimes_{\mathrm{L}}^{\mathcal{N}}\ [\mathrm{TR5}_S \uparrow;\mathrm{TR5}_F \downarrow;\mathrm{TR5}_{PF} \downarrow]\Big)$

Step 2 (ET Reduction):

We obtain the reduced ET models of HVDC transmission system of *Type A* and *Type B* from the generated complete ET models. For example, the complete ET model of HVDC *Type A* ($2^4 \times 3^5 \times 5^2$ test cases) is reduced to 123 test cases, as shown in Figure 3.14 using our formal reduction function $\boxtimes^{\mathcal{N}}$ presented in Section 3.1.2.

Step 3 (ET Partitioning):

Assuming that the required demand 2,690 MW is equally distributed on the HVDC transmission lines (TL_1 and TL_2), a different collection of the ET paths can be obtained by observing different COPT capacity outages from Figure 3.14 as follows:

1. $Pr(Type_{A}\lightning\ Capacity\ Outage\ 1345\ MW) =$
   $\sum_{\mathrm{ET}_{\mathrm{Paths}}}(1, 2, 3, 6, 9, 12, 16, 20, 24, 28, 32, 40, 48, 56, 64, 72, 81, 90, 99, 110)$
2. $Pr(Type_{A}\lightning\ Capacity\ Outage\ 2690\ MW) =$
   $\sum_{\mathrm{ET}_{\mathrm{Paths}}}(4, 5, 7, 8, 10, 11, 13 - 15, 17 - 19, \ldots, 91 - 98, 100 - 109, 111 - 122)$

Formal ET Energy Indices Assessment

Using the Definitions 3.12-3.24 (Section 3.3.1), we can verify the probabilistic capacity outage expressions for all outages for *Type A* and *Type B* as well as all energy indices ASAI, ASUI, ENS, ASCI, LOLE, LOEE, EIR. For instance, we can generate the COPT 1345 MW expression of *Type A* for the Québec-New England system as follows:

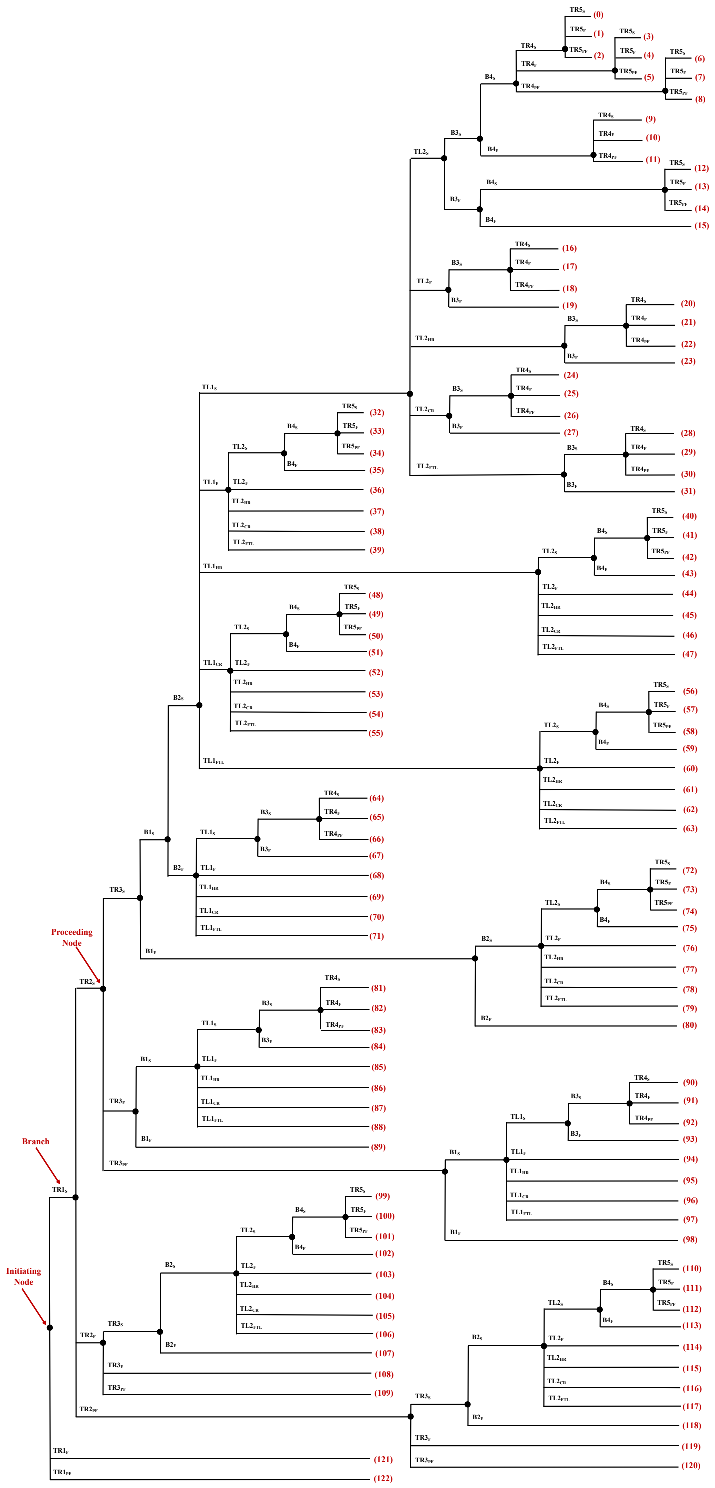


Figure 3.14: Reduced ET of Québec-New England Single Bridge Bipolar System

Theorem 3.10. *Verification of COPT 1345 MW of Type A*

$\vdash$ `COPT_Type_A_Outage_1345_MW =`

$$\Big(\big(\mathrm{e}^{(-\lambda_{TR1_T}t)} \times \mathrm{e}^{(-\lambda_{TR2_T}t)} \times \mathrm{e}^{(-\lambda_{TR3_T}t)} \times \mathrm{e}^{(-\lambda_{B1_F}t)} \times \mathrm{e}^{(-\lambda_{B2_F}t)} \times \mathrm{e}^{(-\lambda_{TL1_T}t)} \times$$
$$\mathrm{e}^{(-\lambda_{TL2_T}t)} \times \mathrm{e}^{(-\lambda_{B3_F}t)} \times \mathrm{e}^{(-\lambda_{B4_F}t)} \times \mathrm{e}^{(-\lambda_{TR4_T}t)} \times (1 - \mathrm{e}^{(-\lambda_{TR5_F}t)})\big) +$$
$$\big(\mathrm{e}^{(-\lambda_{TR1_T}t)} \times \mathrm{e}^{(-\lambda_{TR2_T}t)} \times \mathrm{e}^{(-\lambda_{TR3_T}t)} \times \mathrm{e}^{(-\lambda_{B1_F}t)} \times \mathrm{e}^{(-\lambda_{B2_F}t)} \times \mathrm{e}^{(-\lambda_{TL1_T}t)} \times$$
$$\mathrm{e}^{(-\lambda_{TL2_T}t)} \times \mathrm{e}^{(-\lambda_{B3_F}t)} \times \mathrm{e}^{(-\lambda_{B4_F}t)} \times \mathrm{e}^{(-\lambda_{TR4_T}t)} \times (1 - \mathrm{e}^{(-\lambda_{TR5_{PF}}t)})\big) +$$
$$\big(\mathrm{e}^{(-\lambda_{TR1_T}t)} \times \mathrm{e}^{(-\lambda_{TR2_T}t)} \times \mathrm{e}^{(-\lambda_{TR3_T}t)} \times \mathrm{e}^{(-\lambda_{B1_F}t)} \times \mathrm{e}^{(-\lambda_{B2_F}t)} \times \mathrm{e}^{(-\lambda_{TL1_T}t)} \times$$
$$\mathrm{e}^{(-\lambda_{TL2_T}t)} \times \mathrm{e}^{(-\lambda_{B3_F}t)} \times \mathrm{e}^{(-\lambda_{B4_F}t)} \times (1 - \mathrm{e}^{(-\lambda_{TR4_F}t)}) \times \mathrm{e}^{(-\lambda_{TR5_T}t)}\big) + \ldots +$$
$$\big(\mathrm{e}^{(-\lambda_{TR1_T}t)} \times (1 - \mathrm{e}^{(-\lambda_{TR2_{PF}}t)}) \times \mathrm{e}^{(-\lambda_{TR3_T}t)} \times \mathrm{e}^{(-\lambda_{B2_F}t)} \times \ldots \times \mathrm{e}^{(-\lambda_{TR5_T}t)}\big)$$

where $\lambda_{TRX_T} = \lambda_{TRX_F} + \lambda_{TRX_{PF}}$ and $\lambda_{TLX_T} = \lambda_{TLX_F} + \lambda_{TLX_{HR}} + \lambda_{TLX_{CR}} + \lambda_{TLX_{FTL}}$. Considering the failure rate of the HVDC system components, i.e., λ_B, λ_{TR_F}, $\lambda_{TR_{PF}}$, λ_{TL_F}, $\lambda_{TL_{HR}}$, $\lambda_{TL_{CR}}$, $\lambda_{TL_{FTL}}$, are 0.12, 0.19, 0.09, 0.22, 0.10, 0.06, 0.08 per year with MTTR of 20, 35, 48 hours [76]. Also, assuming the numbers of customers served at Nicolet and Sandy Pond are 50,000 and 65,000 customers, respectively. The reliability study is undertaken for 1 year (365 days), i.e., t = 8760 hours. Therefore, we can evaluate the capacity outage probability table COPT as well as the energy indices ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR for the HVDC system of *Type A* and

Table 3.2: Capacity Outage Probability Table (COPT) of HVDC Coupling

HVDC Capacity			Probability Evaluation		
HVDC Type	Out	In	Manual	MATLAB	HOL4
Type A	0 MW	2690 MW	60.08e-4	55.15e-4	60.07921e-4
	1345 MW	1345 MW	31.16e-2	26.43e-2	31.16378e-2
	2690 MW	0 MW	68.24e-2	73.02e-2	68.23543e-2
Type B	0 MW	2690 MW	98.34e-2	97.05e-2	98.33943e-2
	1345 MW	1345 MW	13.59e-3	20.02e-3	13.58625e-3
	2690 MW	0 MW	30.13e-4	94.08e-4	30.12945e-4
CPU Time			–	5.144 min	20.837 sec

Table 3.3: Energy Indices of HVDC Coupling Types A and B

HVDC Energy Indices	Manual		MATLAB		HOL4	
	Type A	Type B	Type A	Type B	Type A	Type B
ASAI	0.989	0.999	0.962	0.985	0.98852	0.99861
ASUI	0.011	0.001	0.038	0.015	0.01148	0.00139
ENS (MWh)	5652.37	879.75	6215.41	941.23	5652.367	879.746
ASCI (KWh/Cust.yr)	49.15	7.65	54.05	8.18	49.14913	7.64997
LOLE (days/year)	2.19	0.34	2.685	0.41	2.19289	0.34094
LOEE p.u.	0.034	0.001	0.058	0.025	0.03398	0.0019
EIR	0.966	0.999	0.942	0.975	0.96602	0.99881
CPU Time	–		6.204 min		35.315 sec	

Type B using: (1) HOL4 analysis; (2) manual analysis; and (3) MATLAB MCS, which are presented in Tables 3.2 and 3.3, respectively. We run the MATLAB simulation on a single machine, however, using more machines we could analyze the models with faster CPU time. The time taken in modeling the HVDC system using MATLAB was greater than HOL4 (a matter of hours in both cases) but not comparable with the manual method, which took several days. It is evident from the above-obtained energy indices results that our ET formulations can model a complex ET of a HVDC system composed of different *multi-state*-based system components. This shows the superiority of our formal results compared to all existing ET analysis methods.

3.3.4 IEEE 118-Bus Transmission Power Grid

In this third case study, we analyze multiple complex ET models simultaneously corresponding to loads A, B, C of a standard IEEE 118-bus power grid representing a portion of the American electric power system (in the Midwestern US) [78]. The American power grid consists of 19 Generators (G), 186 Transmission Lines (TL), and

91 loads, as shown in Figure 3.15. Using the Optimal Power Flow (OPF) optimization [79], we can determine the flow of power, as shown in Figure 3.15.

Formal Two-State Multiple ET Models

We can formally describe the complex ET models of all TLs that affect the reliability of all loads A, B and C (2048, 1024 and 4096 possible test cases, respectively), using our ET generation function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$, in HOL4 as:

Definition 3.30. *Complete ET Model of IEEE 118-Bus Transmission Load A*

$\vdash$ `IEEE_118_BUS_COMPLETE_ET_LOAD_A =`

`ETREE (NODE`

$(\uparrow\downarrow\ [\mathrm{TL}_1;\mathrm{TL}_2;\mathrm{TL}_3;\mathrm{TL}_4;\mathrm{TL}_5;\mathrm{TL}_6;\mathrm{TL}_7;\mathrm{TL}_8;\mathrm{TL}_9;\mathrm{TL}_{10}])\ \bigotimes_{\mathrm{L}}^{\mathcal{N}}\ (\uparrow\downarrow\ [\mathrm{TL}_{11}]))$

Definition 3.31. *Complete ET Model of IEEE 118-Bus Transmission Load B*

$\vdash$ `IEEE_118_BUS_COMPLETE_ET_LOAD_B =`

`ETREE (NODE`

$(\uparrow\downarrow\ [\mathrm{TL}_{12};\mathrm{TL}_{13};\mathrm{TL}_{14};\mathrm{TL}_{15};\mathrm{TL}_{16};\mathrm{TL}_{17};\mathrm{TL}_{18};\mathrm{TL}_{19};\mathrm{TL}_{20}])\ \bigotimes_{\mathrm{L}}^{\mathcal{N}}\ (\uparrow\downarrow\ [\mathrm{TL}_{21}]))$

Definition 3.32. *Complete ET Model of IEEE 118-Bus Transmission Load C*

$\vdash$ `IEEE_118_BUS_COMPLETE_ET_LOAD_C =`

`ETREE (NODE`

$(\uparrow\downarrow\ [\mathrm{TL}_{22};\mathrm{TL}_{23};\mathrm{TL}_{24};\mathrm{TL}_{25};\ldots;\mathrm{TL}_{29};\mathrm{TL}_{30};\mathrm{TL}_{31};\mathrm{TL}_{32}])\ \bigotimes_{\mathrm{L}}^{\mathcal{N}}\ (\uparrow\downarrow\ [\mathrm{TL}_{33}]))$

Assuming the generators and the transmission lines (TL_1-TL_{33}) are loaded to 90% and 70% of their full capacity, respectively, so that if a sudden TL failure occurs and one of the generators is cut-off, then the power utility can utilize the reservoir in other generators along with the full capacity loading of other TLs to apply around 15% *load-shedding* [80] only, but the failure of two main TLs causes a complete load shutdown, and thereupon the electric utility can maintain the stability [74] of the rest

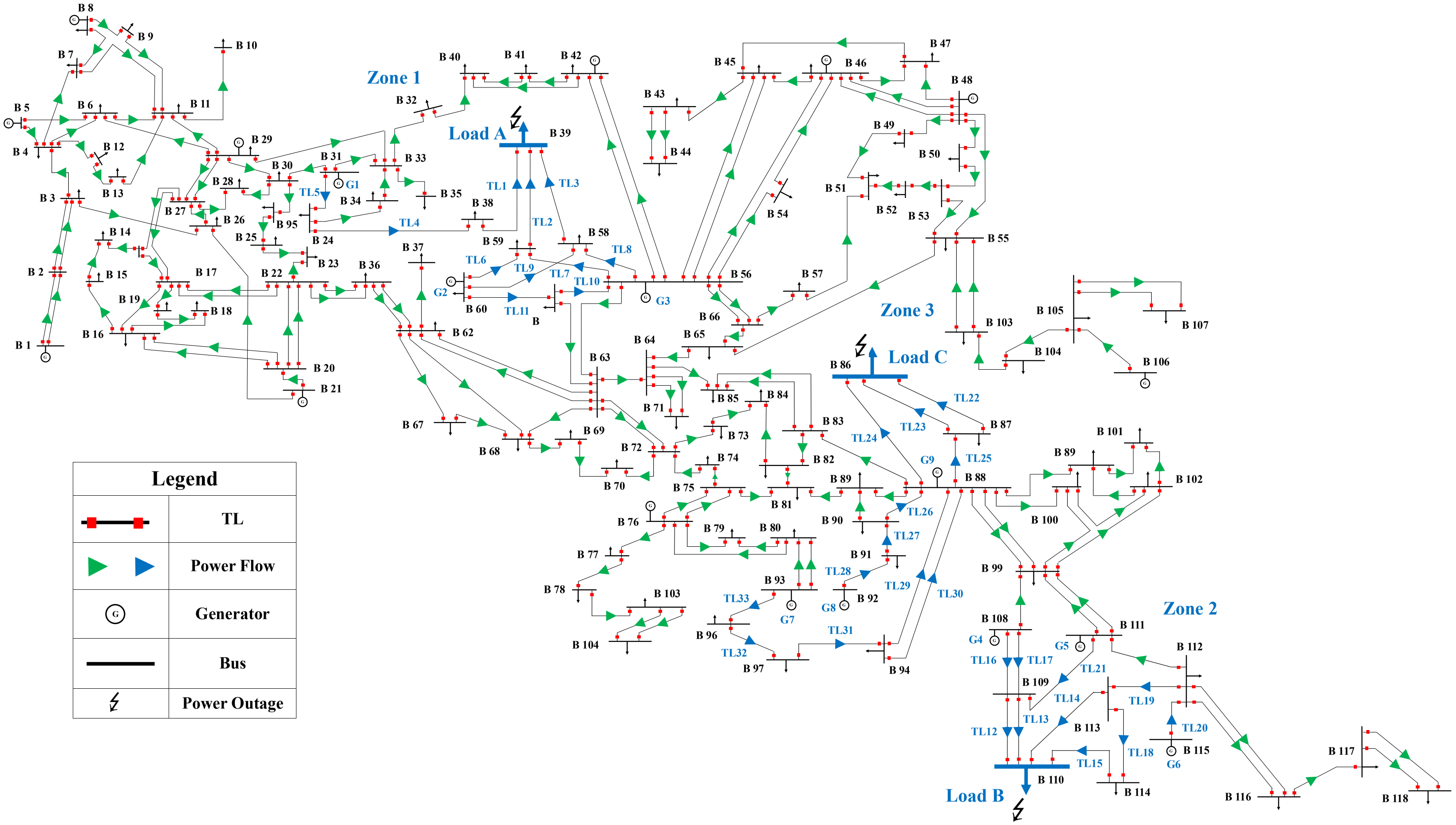


Figure 3.15: IEEE 118-Bus Electrical Power Grid System

of the grid and prevent a complete blackout. Based on the assumption data, we can follow the procedure of *ET reduction* and *ET partitioning* processes for each complex ET model corresponding to all loads to obtain the loads complete/partial failure paths.

Formal ET Reliability Indices Assessment

Using our reliability formulations, we can formally verify the complex expressions of SAIFI, SAIDI, CAIDI for the IEEE 118-bus power system, in HOL4 as [71]:

Theorem 3.11. *Verification of Complex SAIDI for the IEEE 118-bus Grid*

$\vdash$ `SAIDI =`

$$\frac{\begin{array}{l}
\Big(\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \mathrm{e}^{(-\lambda_{TL_3}t)} \times \mathrm{e}^{(-\lambda_{TL_4}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_5}t)}) \times \mathrm{e}^{(-\lambda_{TL_6}t)} \times \\
\quad \mathrm{e}^{(-\lambda_{TL_7}t)} \times \mathrm{e}^{(-\lambda_{TL_8}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) + \dots\Big) \times \mathrm{MTTR}_A \times \mathrm{CN}_A + \\
\Big(\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \mathrm{e}^{(-\lambda_{TL_3}t)} \times \mathrm{e}^{(-\lambda_{TL_4}t)} \times \mathrm{e}^{(-\lambda_{TL_5}t)} \times \mathrm{e}^{(-\lambda_{TL_6}t)} \times \mathrm{e}^{(-\lambda_{TL_7}t)} \times \\
\quad \mathrm{e}^{(-\lambda_{TL_8}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_{10}}t)}) + \dots\Big) \times \mathrm{MTTR}_A \times 15\%\ \mathrm{CN}_A + \\
\Big(\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times \mathrm{e}^{(-\lambda_{TL_{15}}t)} \times \mathrm{e}^{(-\lambda_{TL_{18}}t)} \times \mathrm{e}^{(-\lambda_{TL_{19}}t)} \times \\
\quad \mathrm{e}^{(-\lambda_{TL_{20}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{21}}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_{16}}t)}) + \dots\Big) \times \mathrm{MTTR}_B \times \mathrm{CN}_B + \\
\Big(\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times \mathrm{e}^{(-\lambda_{TL_{15}}t)} \times \mathrm{e}^{(-\lambda_{TL_{18}}t)} \times \mathrm{e}^{(-\lambda_{TL_{19}}t)} \times \\
\quad \mathrm{e}^{(-\lambda_{TL_{20}}t)} \times \mathrm{e}^{(-\lambda_{TL_{21}}t)} \times \cdots \times (1-\mathrm{e}^{(-\lambda_{TL_{17}}t)}) + \dots\Big) \times \mathrm{MTTR}_B \times 15\%\ \mathrm{CN}_B + \\
\Big(\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times \mathrm{e}^{(-\lambda_{TL_{23}}t)}\mathrm{e}^{(-\lambda_{TL_{24}}t)} \times \mathrm{e}^{(-\lambda_{TL_{25}}t)} \times \mathrm{e}^{(-\lambda_{TL_{26}}t)} \times \mathrm{e}^{(-\lambda_{TL_{27}}t)} \times \\
\quad (1-\mathrm{e}^{(-\lambda_{TL_{28}}t)}) \times \mathrm{e}^{(-\lambda_{TL_{29}}t)} \times \mathrm{e}^{(-\lambda_{TL_{30}}t)} \times \mathrm{e}^{(-\lambda_{TL_{31}}t)} \times \mathrm{e}^{(-\lambda_{TL_{32}}t)} \times \\
\quad (1-\mathrm{e}^{(-\lambda_{TL_{33}}t)}) + (1-\mathrm{e}^{(-\lambda_{TL_{22}}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_{23}}t)}) + \dots\Big) \times \mathrm{MTTR}_C \times \mathrm{CN}_C + \\
\Big(\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times \mathrm{e}^{(-\lambda_{TL_{23}}t)}\mathrm{e}^{(-\lambda_{TL_{24}}t)} \times \mathrm{e}^{(-\lambda_{TL_{25}}t)} \times \mathrm{e}^{(-\lambda_{TL_{26}}t)} \times \mathrm{e}^{(-\lambda_{TL_{27}}t)} \times \\
\quad \mathrm{e}^{(-\lambda_{TL_{28}}t)} \times \mathrm{e}^{(-\lambda_{TL_{29}}t)} \times \mathrm{e}^{(-\lambda_{TL_{30}}t)} \times \mathrm{e}^{(-\lambda_{TL_{31}}t)} \times \mathrm{e}^{(-\lambda_{TL_{32}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{33}}t)}) + \\
\quad \mathrm{e}^{(-\lambda_{TL_{22}}t)}\mathrm{e}^{(-\lambda_{TL_{23}}t)} \times \cdots \times (1-\mathrm{e}^{(-\lambda_{TL_{25}}t)}) + \dots\Big) \times \mathrm{MTTR}_C \times 15\%\ \mathrm{CN}_C
\end{array}}{\mathrm{CN}_A + \mathrm{CN}_B + \mathrm{CN}_C}$$

Similarly, we verify the SAIFI and CAIDI indices for two-state multiple ET models of 118-bus electrical grid. Considering the failure rates λ_{TL_1}-λ_{TL_4}, λ_{TL_5}-λ_{TL_8}, λ_{TL_9}-$\lambda_{TL_{11}}$, $\lambda_{TL_{12}}$-$\lambda_{TL_{15}}$, $\lambda_{TL_{16}}$-$\lambda_{TL_{18}}$, $\lambda_{TL_{19}}$-$\lambda_{TL_{21}}$, $\lambda_{TL_{22}}$-$\lambda_{TL_{25}}$, $\lambda_{TL_{26}}$-$\lambda_{TL_{29}}$, $\lambda_{TL_{30}}$-$\lambda_{TL_{33}}$ are 0.2, 0.5, 0.3, 0.25, 0.4, 0.15, 0.35, 0.29, 0.45 per year with an average MTTR of 30 hours [78]. Also assuming the number of customers CN_A, CN_B and CN_C to be 12,000, 9,000 and 11,000 customers, respectively. The reliability study is undertaken for 5 years, i.e., $t = (8760 \times 5)$ hours. Therefore, we can evaluate SAIFI, SAIDI and CAIDI for the 118-bus grid using: (1) HOL4 analysis; (2) Isograph software; (3) MATLAB MCS; and (4) paper-and-pencil analysis. A comparison between all methods is presented in Table 3.4. It can be noticed the slight difference of Isograph results compared to our formal analysis and manual analysis due to the approximation in computing results in Isograph. It took several hours to build the models of the 118-bus using the Isograph and MATLAB tools, respectively, but HOL4 was less time consuming than both. In contrast, the modeling for the manual analysis required a few days to complete.

Table 3.4: Comparison of 118-Bus Transmission SAIFI, SAIDI and CAIDI

IEEE 118-Bus Transmission Reliability Indices	Manual	Isograph	MATLAB	HOL4
SAIFI (Interruptions/Customer)	0.65695	0.6579	0.7267	0.656948446
SAIDI (Hours/Customer)	19.70845	19.8592	24.5282	19.708453419
CAIDI (Hours/Customer Interruption)	29.99991	30.1857	33.7541	30.000000000
CPU Time (Seconds)	–	47.205	153.916	9.477

The above-obtained experimental reliability indices validate the scalability of our proposed ET formalization in HOL4 for handling separated complex ET load models simultaneously and generating the complex expressions of different reliability indices of the entire power grid for all loads (e.g., Theorem 3.11) with more accurate results and in much less CPU time with respect to all existing analysis methods.

3.4 Summary

In this chapter, we presented the formalization of ET step-wise analysis. We developed a new ET datatype `EVENT_TREE` with the basic ET constructors and formalized generic functions that can generate the mathematical ET model of two stair and $\mathcal{N}$ stairs. Furthermore, we formalized generic functions that can perform the ET reduction and partitioning, respectively. We verified the related probabilistic formulations for ET nodes, branches, paths and multiple paths. The proofs in HOL4 required multiple levels of induction and were based on several HOL4 theories, such as measure theory, probability theory, set theory, list theory, arithmetic theory, real theory and extended real theory. The proof-script of the above ET formalizations and theorems amounts to about 4,000 lines of HOL4 code, which can be downloaded from [71]. Based on the verified ET probabilistic formulations, we established a formal ET analysis process, which we applied on different complexity ET levels of realistic power systems and determined significant reliability and energy indices. The experimental formal results were validated by comparing them with all available ET based analysis methods.

In many realistic complex systems, the central safety inquiry is to identify the possible consequences given that one or more sudden event could happen at the subsystem level. For that purpose, we propose the formalization of CCDs in the next chapter. CCD reliability analysis is used to analyze failures at the subsystem levels using FTs combined with an ET consequence diagram to integrate their cascading failure/reliability dependencies on the entire system. In Chapter 4, we provide the formalization of the state-of-the-art CCDs using FTs and ETs, which enables safety analysts to perform formal failure analysis for multi-level subsystems.

Chapter 4

Formal FT-based Cause Consequence Reliability Analysis

In this chapter, we present the detailed formalization of cause-consequence reliability analysis of safety-critical systems in HOL4, using a combination of the existing formalization of Fault Trees (FT) in HOL4 (Section 2.4) and our formalization of Event Trees (ET) proposed in Chapter 3. We endeavor to formalize in HOL4 the four steps of CCD analysis, i.e., *Subsystems failure events*, *Construction of a complete CCD*, *CCD Reduction* and *CCD Probabilistic analysis* (see Section 2.3). We propose novel formulations that can analyze *multi-level* cause consequence analysis of realistic complex systems at the subsystem level. Lastly, an application on an IEEE 39-bus distributed generation network is presented.

4.1 CCD Formalization

We start the formalization of CDDs by formally modeling its basic constructing symbols, as described in Table 2.1 in HOL4 as follows:

Definition 4.1. *CCD Decision Box*

$\vdash$ DEC_BOX p X Y =

if X = 1 then FST Y else if X = 0 then SND Y else p_space p

where Y is an ordered pair (FST Y, SND Y) representing the reliability and unreliability functions in a decision box, respectively. The condition X = 1 represents the YES Box while X = 0 represents the NO Box. If X is neither 1 nor 0, for instance, X = 2, this represents the irrelevance of the decision box, which returns the probability space *p* to be used in the reduction process of CCDs.

Secondly, we define the CCD *Consequence path* by recursively applying the BRANCH ET constructor on a given $\mathcal{N}$ list of decision boxes (DEC_BOX$_{\mathcal{N}}$) using the HOL4 recursive function FOLDL as:

Definition 4.2. *CCD Consequence Path*

$\vdash$ CONSEQ_PATH p (DEC_BOX$_1$::DEC_BOX$_{\mathcal{N}}$) =

FOLDL (λa b. ETREE (BRANCH a b)) DEC_BOX$_1$ DEC_BOX$_{\mathcal{N}}$

Finally, we define the *Consequence box* by mapping the function CONSEQ_PATH on a given *two-dimensional* list of consequence paths L$_{\mathcal{M}}$ using the HOL4 mapping function MAP, then applying the NODE ET constructor:

Definition 4.3. *CCD Consequence Box*

$\vdash$ CONSEQ_BOX p L$_{\mathcal{M}}$ = ETREE (NODE (MAP (λa. CONSEQ_PATH p a) L$_{\mathcal{M}}$))

Using the above definitions, we can construct a complete CCD model for the PV solar system shown in Figure 2.6(a) (see Section 2.3), in HOL4 as:

Definition 4.4. *Complete CCD Model of Solar PV System*

$\vdash$ Solar_PV_Complete_CCD FT_{SA} FT_{IB} =

CONSEQ_BOX p [[DEC_BOX p 1 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 1 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)];
[DEC_BOX p 1 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 0 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)];
[DEC_BOX p 0 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 1 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)];
[DEC_BOX p 0 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 0 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)]]

The next step in CCD analysis [29], *Step 3* is used to reduced the number of possible test cases. Upon this, the actual CCD model of the PV solar system after reduction, as shown in Figure 2.6(b), can be obtained by assigning X with neither 1 nor 0, for instance, X = 2, in HOL4 as:

Definition 4.5. *Reduced CCD Model of Solar PV System*

$\vdash$ Solar_PV_Reduced_CCD FT_{SA} FT_{IB} =

CONSEQ_BOX p [[DEC_BOX p 1 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 1 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)];
[DEC_BOX p 1 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 0 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)];
[DEC_BOX p 0 ($\overline{\mathrm{FT}_{SA}}$,$\mathrm{FT}_{SA}$); DEC_BOX p 2 ($\overline{\mathrm{FT}_{IB}}$,$\mathrm{FT}_{IB}$)]]

where $\overline{\mathrm{FT}_X}$ for a subsystem X is the complement of FT_X using the NOT gate.

4.2 Formal FT-based CCD Analysis

The important step in the CCD analysis is to determine the probability of each consequence path occurrence in the CCD [27]. For that purpose, we formally verify the following CCD *generic* probabilistic properties.

One CCD Decision Box

Figure 4.1 depicts one CCD decision box associated with a *generic* AND or OR FT model. If the connected FT model is AND, then the outcome is equal to Equation 2.8 if the decision is 0 (failure) while the outcome is equal to the complement of Equation 2.8 if the decision is 1 (success). Similarly, if the connected FT model is OR, then the outcome is equal to Equation 2.9 or the complement of Equation 2.9 if the decision is 0 or 1, respectively. We formalize the probability of a consequence path for *one* decision box, in HOL4 as:

Theorem 4.1. *One Subsystem Decision Box of OR Configuration*

$\vdash \texttt{prob p}$

$\quad\Big(\texttt{CONSEQ\_PATH p}$

$\qquad\big[\texttt{DEC\_BOX p X } \big(\texttt{FTree p (NOT (OR F}_K\texttt{)), FTree p (OR F}_K\texttt{))}\big]\big]\Big)$

$\quad\texttt{= if X = 1 then } \prod \Big(\mathrm{Pr}_\mathrm{L}\texttt{ p (COMPL\_LIST p F}_K\texttt{)}\Big)$

$\quad\;\texttt{else if X = 0 then 1 - } \prod \Big(\mathrm{Pr}_\mathrm{L}\texttt{ p (COMPL\_LIST p F}_K\texttt{)}\Big)\texttt{ else 1}$

Theorem 4.2. *One Subsystem Decision Box of AND Configuration*

$\vdash \texttt{prob p}$

$\quad\Big(\texttt{CONSEQ\_PATH p}$

$\qquad\quad\big[\texttt{DEC\_BOX p X } \big(\texttt{FTree p (NOT (AND F}_J\texttt{)),FTree p (AND F}_J\texttt{))}\big]\big]\Big)$

$\quad\texttt{= if X = 1 then 1 - } \prod \texttt{ (}\mathrm{Pr}_\mathrm{L}\texttt{ p F}_J\texttt{)}$

$\quad\;\texttt{else if X = 0 then } \prod \texttt{ (}\mathrm{Pr}_\mathrm{L}\texttt{ p F}_J\texttt{) else 1}$

To have a clear understanding, consider the 3 PV solar array (Figure 2.5) are connected in series to increase the outcome voltage, as shown in Figure 4.2(a). Therefore, the solar system fails if any PV fails. We can formally model FT$_{Solar}$, in HOL4 as:

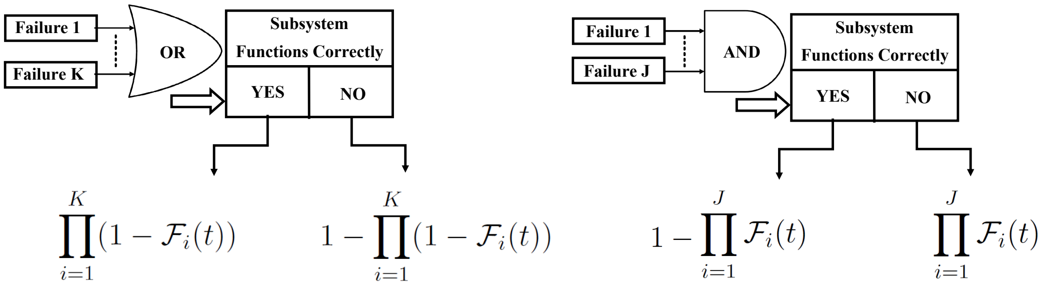
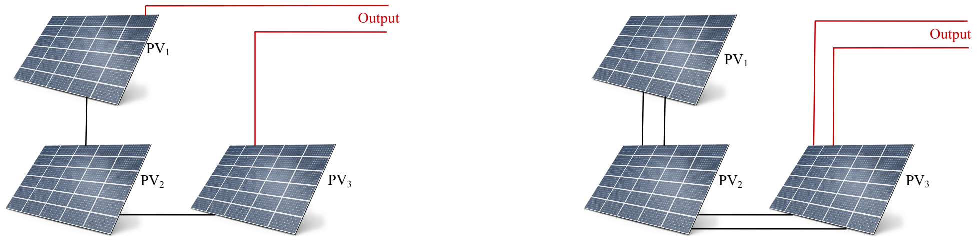

Failure 1
Failure K
OR
Subsystem Functions Correctly
YES
NO
$\prod_{i=1}^{K}(1-\mathcal{F}_i(t))$
$1-\prod_{i=1}^{K}(1-\mathcal{F}_i(t))$
Failure 1
Failure J
AND
Subsystem Functions Correctly
YES
NO
$1-\prod_{i=1}^{J}\mathcal{F}_i(t)$
$\prod_{i=1}^{J}\mathcal{F}_i(t)$

Figure 4.1: Decision Boxes with FT AND and OR Gates



(a) Series PVs Connection (b) Parallel PVs Connection

Figure 4.2: Solar Photo-Voltaic (PV) Connections

Definition 4.6. *Solar Photo-Voltaic Series Panels Configuration*

⊢ FT_{Solar} p PV_{1F} PV_{2F} PV_{3F} = FTree p (OR [PV_{1F};PV_{2F};PV_{3F}])

Using Theorem 4.1, we can obtain the probability of a decision box `YES/NO` outcomes connected to the above series solar FT model, respectively, in HOL4 as:

Theorem 4.3. *Probabilistic YES Outcome of Series Solar Decision Box*

⊢ prob p (CONSEQ_PATH p [DEC_BOX p 1 ($\overline{\mathrm{FT}_{Solar}}$,$\mathrm{FT}_{Solar}$))]) =

(1 - $Pr(\mathrm{PV}_{1F})$) × (1 - $Pr(\mathrm{PV}_{2F})$) × (1 - $Pr(\mathrm{PV}_{3F})$)

Theorem 4.4. *Probabilistic NO Outcome of Series Solar Decision Box*

⊢ prob p (CONSEQ_PATH p [DEC_BOX p 0 ($\overline{\mathrm{FT}_{Solar}}$,$\mathrm{FT}_{Solar}$))]) =

1 - (1 - $Pr(\mathrm{PV}_{1F})$) × (1 - $Pr(\mathrm{PV}_{2F})$) × (1 - $Pr(\mathrm{PV}_{3F})$)

If the panels are connected in parallel to increase the outcome current, as shown in Figure 4.2(b), then the solar system fails only if all PVs fail simultaneously. We can formally model FT_{Solar}, in HOL4 as follows:

Definition 4.7. *Solar Photo-Voltaic Parallel Panels Configuration*

⊢ FT_{Solar} p PV_{1F} PV_{2F} PV_{3F} = FTree p (AND [PV_{1F};PV_{2F};PV_{3F}])

Using Theorem 4.2, we can obtain the probability of a decision box `YES/NO` outcomes connected to the above parallel solar FT model, respectively, in HOL4 as:

Theorem 4.5. *Probabilistic YES Outcome of Parallel Solar Decision Box*

$\vdash$ `prob p (CONSEQ_PATH p [DEC_BOX p 1 (`$\overline{\mathrm{FT}_{Solar}}$`,`$\mathrm{FT}_{Solar}$`))]) =`

`1 -` $Pr(\mathrm{PV}_{1F}) \times Pr(\mathrm{PV}_{2F}) \times Pr(\mathrm{PV}_{3F})$

Theorem 4.6. *Probabilistic NO Outcome of Parallel Solar Decision Box*

$\vdash$ `prob p (CONSEQ_PATH p [DEC_BOX p 0 (`$\overline{\mathrm{FT}_{Solar}}$`,`$\mathrm{FT}_{Solar}$`))]) =`

$Pr(\mathrm{PV}_{1F}) \times Pr(\mathrm{PV}_{2F}) \times Pr(\mathrm{PV}_{3F})$

Now, we propose a solution for *multi-level* CCD reliability analysis for realistic complex systems consisting of multi-level decision boxes corresponding to connected multi-level subsystems, where each subsystem is analyzed by different AND/OR gates associated with an arbitrary list of failure events, i.e., *multi-level* FT models and *multi-level* ET model, as shown in Figure 4.3. Note that the work of Ridley [9] for FT

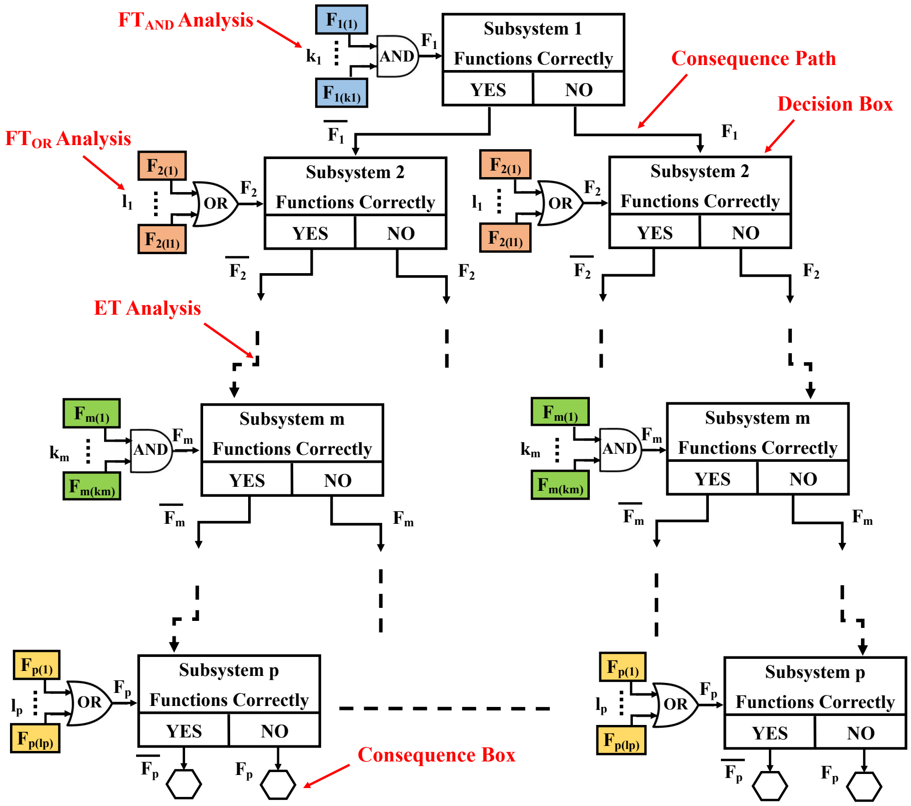


Figure 4.3: Generic Multi-Level FT/ET-based Cause Consequence Analysis

based CCD analysis is unable to analyze such generic multilevel models since it is done manually using paper-and-pencil approach for concrete instances of the CCD decision boxes. It can be noticed from Figure 4.3 that the output of each `NO BOX` for all decision boxes is equal to the subsystem FT model ($\mathrm{FT_X}$), while the `YES BOX` is the complement of the FT model ($\overline{\mathrm{FT_X}}$). Therefore, in order to have probabilistic expressions for all CCD paths of multi-level decision boxes, we define *three* types A, B and C of possible CCD path outcomes, which are presented in the next subsections, respectively.

N CCD Decision Boxes of Type A

The probabilistic risk assessment of n decision boxes assigned to a consequence path corresponding to n subsystems, where all decision boxes are associated with FT AND models consisting of different arbitrary lists of k events, as shown in Figure 4.4, can be expressed mathematically at a specific time t for *three* cases as:

(A1) All outcomes of n decisions boxes are NO

$$\mathcal{F}_{A1}(t) = \prod_{i=1}^{n}\prod_{j=1}^{k}\mathcal{F}_{ij}(t) \tag{4.1}$$

(A2) All outcomes of n decisions boxes are YES

$$\mathcal{F}_{A2}(t) = \prod_{i=1}^{n}(1 - \prod_{j=1}^{k}\mathcal{F}_{ij}(t)) \tag{4.2}$$

(A3) Some outcomes of m out of n decisions boxes are NO and some outcomes of p out of n decisions boxes are YES

$$\mathcal{F}_{A3}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{F}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}(1 - \prod_{j=1}^{k}\mathcal{F}_{ij}(t))\right) \tag{4.3}$$

To verify the correctness of the above-proposed new safety analysis mathematical formulations in the HOL4 theorem prover, we define two generic CCD functions $\mathcal{SS}_{AND}^{YES}$ and $\mathcal{SS}_{AND}^{NO}$ that can recursively generate the outcomes YES and NO of the

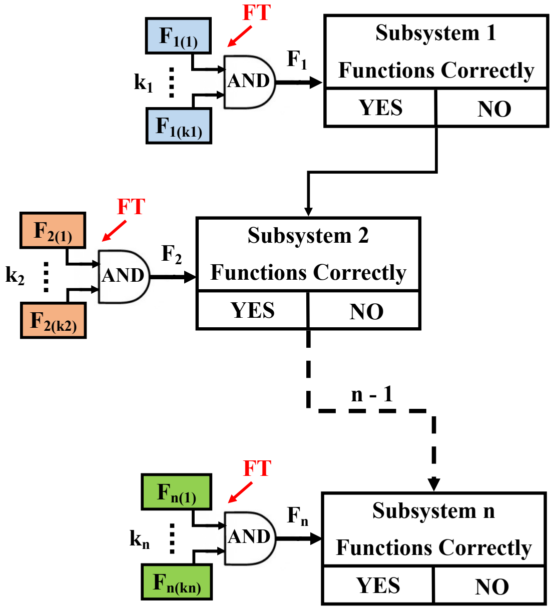


Figure 4.4: Multi-Level Failure Analysis of Type A

function `FTree`, identified by `gate` constructors `AND` and `NOT`, for a given arbitrary list of all subsystems (SS) failure events, respectively, in HOL4 as follows:

Definition 4.8. *Multi-Level AND Decision Boxes of YES Outcomes*

$\vdash \mathcal{SS}^{YES}_{AND}$ `p (SS1::SSN) = FTree p (NOT (AND SS1))::`$\mathcal{SS}^{YES}_{AND}$ `p SSN`

Definition 4.9. *Multi-Level AND Decision Boxes of NO Outcomes*

$\vdash \mathcal{SS}^{NO}_{AND}$ `p (SS1::SSN) = FTree p (AND SS1)::`$\mathcal{SS}^{NO}_{AND}$ `p SSN`

Using above defined functions, we can verify three two-dimensional probabilistic properties corresponding to the above-mentioned safety Equations 4.1, 4.2 and 4.3, respectively, in HOL4 as:

Theorem 4.7. *Probability of Multi-Level AND Decision Boxes with All NO*

$$\vdash \texttt{prob p } \Big(\texttt{CONSEQ\_PATH p } (\mathcal{SS}^{NO}_{AND}\texttt{ p SSN}) = \prod \texttt{ (MAP } (\lambda\texttt{ a. } \prod \texttt{ (Pr}_{\texttt{L}}\texttt{ p a)) SSN}\Big)$$

Theorem 4.8. *Probability of Multi-Level AND Decision Boxes with All YES*

$$\vdash \texttt{prob p } \Big(\texttt{CONSEQ\_PATH p } (\mathcal{SS}^{YES}_{AND}\texttt{ p SSN}) = \prod \texttt{ (MAP } (\lambda\texttt{ b. } (1 - \prod \texttt{ (Pr}_{\texttt{L}}\texttt{ p b))) SSN}\Big)$$

Theorem 4.9. *Probability of Multi-Level AND Decision Boxes with NO/YES*

$\vdash$ `prob p`

$\Big($`CONSEQ_PATH p`

`[CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{AND}$` p SSm); CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{AND}$` p SSp)]`$\Big)$ `=`

$\Big(\prod$ `(MAP (`λ `a.` $\prod$ `(`$\mathrm{Pr_L}$ `p a)) SSm)`$\Big) \times$

$\Big(\prod$ `(MAP (`λ `b. 1 -` $\prod$ `(`$\mathrm{Pr_L}$ `p b)) SSp)`$\Big)$

N CCD Decision Boxes of Type B

The probabilistic risk assessment of n decision boxes assigned to a CCD path, where all decision boxes are associated with generic FT OR models consisting of different arbitrary lists of k events, as shown in Figure 4.5, can be expressed mathematically for *three* cases :

(B1) All outcomes of n decisions boxes are NO

$$\mathcal{F}_{B1}(t) = \prod_{i=1}^{n}(1 - \prod_{j=1}^{k}(1 - \mathcal{F}_{ij}(t))) \tag{4.4}$$

(B2) All outcomes of n decisions boxes are YES

$$\mathcal{F}_{B2}(t) = \prod_{i=1}^{n}\prod_{j=1}^{k}(1 - \mathcal{F}_{ij}(t)) \tag{4.5}$$

(B3) Some outcomes of m out of n decisions boxes are NO and some outcomes of p out of n decisions boxes are YES

$$\mathcal{F}_{B3}(t) = \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}(1 - \mathcal{F}_{ij}(t)))\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{k}(1 - \mathcal{F}_{ij}(t))\right) \tag{4.6}$$

To verify the correctness of the above-proposed new CCD mathematical formulas in HOL4, we define two generic functions $\mathcal{SS}^{YES}_{OR}$ and $\mathcal{SS}^{NO}_{OR}$ to recursively generate

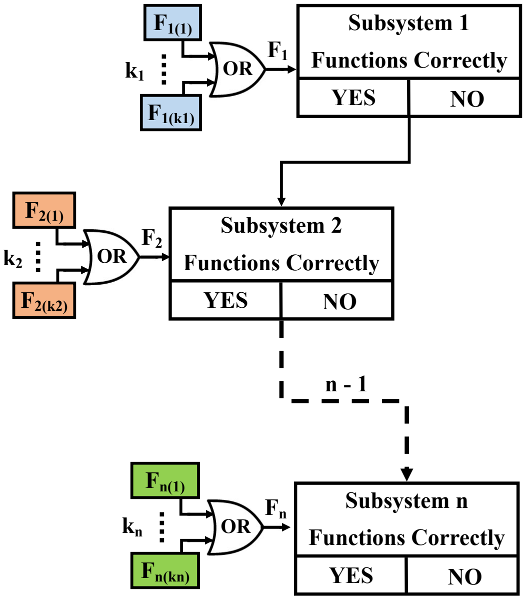


Figure 4.5: Multi-Level Failure Analysis of Type B

the outcomes YES and NO of the function FTree, identified by gate constructors OR and NOT, for a given list of subsystems events.

Definition 4.10. *Multi-Level OR Decision Boxes of YES Outcomes*

$\vdash$ $\mathcal{SS}^{YES}_{OR}$ p (SS1::SSN) = FTree p (NOT (OR SS1))::$\mathcal{SS}^{YES}_{OR}$ p SSN

Definition 4.11. *Multi-Level OR Decision Boxes of NO Outcomes*

$\vdash$ $\mathcal{SS}^{NO}_{OR}$ p (SS1::SSN) = FTree p (OR SS1)::$\mathcal{SS}^{NO}_{OR}$ p SSN

Using above functions, we can formally verify three two-dimensional probabilistic properties corresponding to Equations 4.4, 4.5, and 4.6, respectively, in HOL4 as:

Theorem 4.10. *Probability of Multi-Level OR Decision Boxes with All NO*

$\vdash$ prob p (CONSEQ_PATH p ($\mathcal{SS}^{NO}_{OR}$ p SSN)) =

$\prod$ (MAP (λ a. (1 - $\prod$ (Pr$_\mathrm{L}$ p (compl_list p a)))) SSN)

Theorem 4.11. *Probability of Multi-Level OR Decision Boxes with All YES*

$\vdash$ prob p (CONSEQ_PATH p ($\mathcal{SS}^{YES}_{OR}$ p SSN)) =

$\prod$ (MAP (λ b. $\prod$ (Pr$_\mathrm{L}$ p (compl_list p b))) SSN)

Theorem 4.12. *Probability of Multi-Level OR Decision Boxes with NO/YES*

$\vdash$ `prob p`

`(CONSEQ_PATH p`

`[CONSEQ_PATH p (`$\mathcal{SS}_{OR}^{NO}$` p SSm); CONSEQ_PATH p (`$\mathcal{SS}_{OR}^{YES}$` p SSp)]) =`

$\Big(\prod$ `(MAP (`λ` a. (1 - `$\prod$` (`$\mathrm{Pr_L}$` p (compl_list p a)))) SSm)`$\Big)$ $\times$

$\Big(\prod$ `(MAP (`λ` b. `$\prod$` (`$\mathrm{Pr_L}$` p (compl_list p b))) SSp)`$\Big)$

N CCD Decision Boxes of Type C

The probabilistic risk assessment of multi-level decision boxes assigned to a CCD path for a complex system, where some m decision boxes are associated with FT AND models consisting of different k events, while other p decision boxes are associated with FT OR models consisting of different l events, as shown in Figure 4.3, can be expressed mathematically for *nine* cases as:

(C1) All outcomes of m and p decisions boxes are NO.

$$\mathcal{F}_{C1}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{F}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}(1 - \prod_{j=1}^{l}(1 - \mathcal{F}_{ij}(t)))\right) \tag{4.7}$$

(C2) All outcomes of m and p decisions boxes are YES.

$$\mathcal{F}_{C2}(t) = \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}\mathcal{F}_{ij}(t))\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{l}(1 - \mathcal{F}_{ij}(t))\right) \tag{4.8}$$

(C3) All outcomes of m decisions boxes are NO and all outcomes of p decisions boxes are YES.

$$\mathcal{F}_{C3}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{F}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{l}(1 - \mathcal{F}_{ij}(t))\right) \tag{4.9}$$

(C4) All outcomes of m decisions boxes are YES and all outcomes of p decisions boxes are NO.

$$\mathcal{F}_{C4}(t) = \left(\prod_{i=1}^{m} (1 - \prod_{j=1}^{k} \mathcal{F}_{ij}(t)) \right) \times \left(\prod_{i=1}^{p} (1 - \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t))) \right) \tag{4.10}$$

(C5) Some outcomes of s out of m decisions boxes are NO, some outcomes of u out of m decisions boxes are YES and all outcomes of p decisions boxes are NO.

$$\mathcal{F}_{C5}(t) = \left(\prod_{i=1}^{s} \prod_{j=1}^{k} \mathcal{F}_{ij}(t) \right) \times \left(\prod_{i=1}^{u} (1 - \prod_{j=1}^{k} \mathcal{F}_{ij}(t)) \right) \times \left(\prod_{i=1}^{p} (1 - \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t))) \right) \tag{4.11}$$

(C6) Some outcomes of s out of m decisions boxes are NO, some outcomes of u out of m decisions boxes are YES and all outcomes of p decisions boxes are YES.

$$\mathcal{F}_{C6}(t) = \left(\prod_{i=1}^{s} \prod_{j=1}^{k} \mathcal{F}_{ij}(t) \right) \times \left(\prod_{i=1}^{u} (1 - \prod_{j=1}^{k} \mathcal{F}_{ij}(t)) \right) \times \left(\prod_{i=1}^{p} \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t)) \right) \tag{4.12}$$

(C7) Some outcomes of v out of p decisions boxes are NO, some outcomes of w out of p decisions boxes are YES and all outcomes of m decisions boxes are NO.

$$\mathcal{F}_{C7}(t) = \left(\prod_{i=1}^{v} (1 - \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t))) \right) \times \left(\prod_{i=1}^{w} \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t)) \right) \times \left(\prod_{i=1}^{m} \prod_{j=1}^{k} \mathcal{F}_{ij}(t) \right) \tag{4.13}$$

(C8) Some outcomes of v out of p decisions boxes are NO, some outcomes of w out of p decisions boxes are YES and all outcomes of m decisions boxes are YES.

$$\mathcal{F}_{C8}(t) = \left(\prod_{i=1}^{v} (1 - \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t))) \right) \times \left(\prod_{i=1}^{w} \prod_{j=1}^{l} (1 - \mathcal{F}_{ij}(t)) \right) \times \left(\prod_{i=1}^{m} (1 - \prod_{j=1}^{k} \mathcal{F}_{ij}(t)) \right) \tag{4.14}$$

Using Theorems 4.7-4.12, we formally verify in HOL4 all the above-newly proposed formulas from Equation 4.7 to Equation 4.14 for FT/ET-based cause consequence analysis, which is evidence for the correctness of our proposed formulations.

(C9) Some outcomes of s out of m decisions boxes are NO, some outcomes of u out of m decisions boxes are YES, some outcomes of v out of p decisions boxes are NO and some outcomes of w out of p decisions boxes are YES.

$$\begin{aligned}\mathcal{F}_{C9}(t) =& \left(\prod_{i=1}^{s}\prod_{j=1}^{k}\mathcal{F}_{ij}(t)\right) \times \left(\prod_{i=1}^{u}(1 - \prod_{j=1}^{k}\mathcal{F}_{ij}(t))\right) \times \\ & \left(\prod_{i=1}^{v}(1 - \prod_{j=1}^{l}(1 - \mathcal{F}_{ij}(t)))\right) \times \left(\prod_{i=1}^{w}\prod_{j=1}^{l}(1 - \mathcal{F}_{ij}(t))\right)\end{aligned} \tag{4.15}$$

Theorem 4.13. *Multi-Level Subsystems of OR/AND Decision Boxes with NO/YES*

```
⊢ prob p
     (CONSEQ_PATH p
        [CONSEQ_PATH p ($\mathcal{SS}^{NO}_{AND}$ p SSs); CONSEQ_PATH p ($\mathcal{SS}^{YES}_{AND}$ p SSu);
         CONSEQ_PATH p ($\mathcal{SS}^{NO}_{OR}$ p SSv); CONSEQ_PATH p ($\mathcal{SS}^{YES}_{OR}$ p SSw)]) =
     ($\prod$ (MAP ($\lambda$ a.  $\prod$ ($\mathrm{Pr_L}$ p a)) SSs)) ×
     ($\prod$ (MAP ($\lambda$ b.  1 - $\prod$ ($\mathrm{Pr_L}$ p b)) SSu)) ×
     ($\prod$ (MAP ($\lambda$ c.  (1 - $\prod$ ($\mathrm{Pr_L}$ p (compl_list p c)))) SSv)) ×
     ($\prod$ (MAP ($\lambda$ d.  $\prod$ ($\mathrm{Pr_L}$ p (compl_list p d))) SSw))
```

By verifying all the above-mentioned novel formulations in HOL4, we showed the completeness of our proposed formal approach and thereupon solving the scalability problem of *multi-level* cause consequence analysis for any given large engineering complex system at the subsystem level, which is the first of its kind. Lastly, we need a generic probabilistic property of CONSEQ_BOX for a certain event occurrence in the entire system. For that purpose, we verified in HOL4 the probabilistic expression of CONSEQ_BOX is equal to the sum of all individual probabilities of all $\mathcal{M}$ CONSEQ_PATH ending with that event as follows:

Theorem 4.14. *Probability of Consequence Box for $\mathcal{M}$ Consequence Paths*

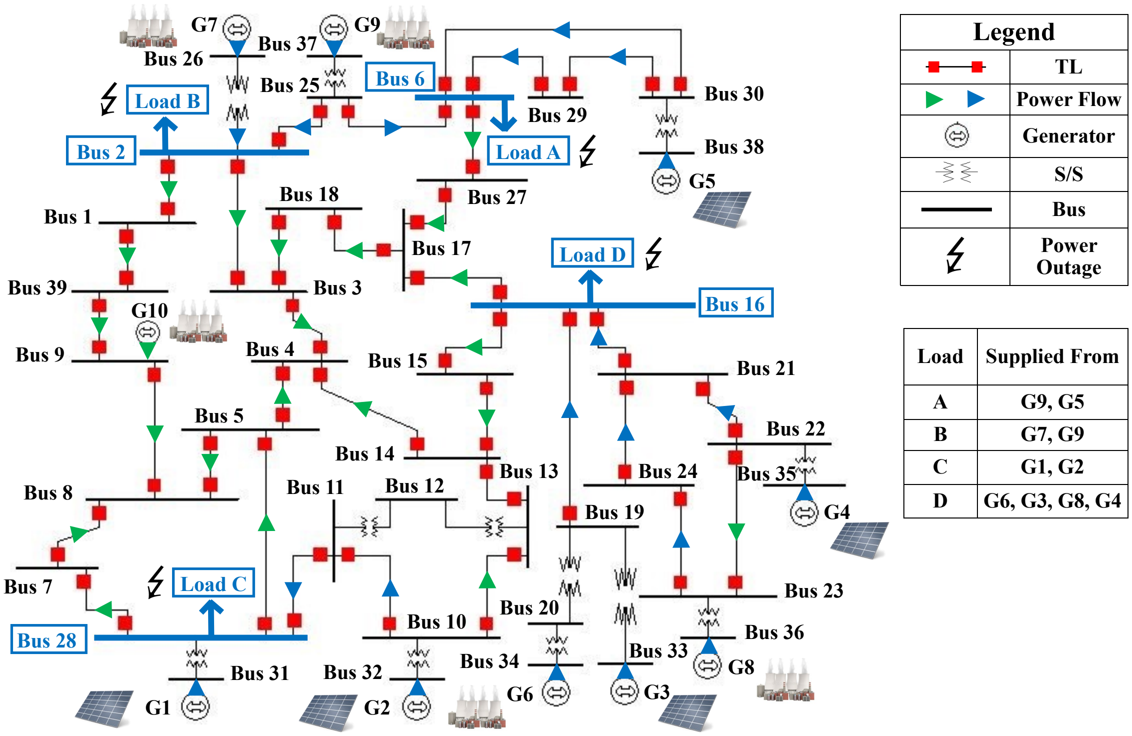
$$\vdash \texttt{prob p (CONSEQ\_BOX p } \mathrm{L}_{\mathcal{M}}\texttt{) =}$$
$$\sum \Big(\mathrm{Pr}_{\mathrm{L}} \texttt{ p (MAP (}\lambda\texttt{a. CONSEQ\_PATH p a) } \mathrm{L}_{\mathcal{M}}\texttt{))}\Big)$$

Remark that the verification of all the above-mentioned theorems was a bit challenging as we are dealing with all four types of different FT configurations, i.e., AND, NAND, OR and NOR, where each type is consisting of *generic* n decision boxes and each decision box is associated with *generic* m events, simultaneously in HOL4. So, we had to verify first *multi-level* connection of ANDs, NANDs, ORs, NORs, then all combinations of each two types together, e.g., *multi-level* of ANDs and *multi-level* of NANDs. Finally, we verified all combinations of each three types together.

To illustrate the applicability of our proposed CCD formalization, in the next section, we present the formal FT-based cause consequence analysis of the standard IEEE 39-bus electrical power generation network and verify the force outage rate (FOR) for all power plants as well as the system average interruption duration index (SAIDI) at each generation subsystem level, which are important to the power utilities.

4.3 Application: IEEE 39-Bus Distributed Generation Network

Consider the standard IEEE 39-bus electrical power generation network consisting of 10 generators (G), 12 substations (S/S), 39 Buses (Bus), and 34 transmission lines (TL), as shown in Figure 4.6 [81].



Load	Supplied From
A	G9, G5
B	G7, G9
C	G1, G2
D	G6, G3, G8, G4

Figure 4.6: IEEE 39-bus Electrical Power Network

In this application, we focus on the distributed generation of 50% truly carbon-neutral or emissions-free [82] green power generation, i.e., Hierarchical level I. Therefore, we assume that the generators G1-G10 are of two types: (i) solar photo-voltaic (PV) power plants G1-G5; and (ii) steam power plants G6-G10. Using the Optimal Power Flow (OPF) optimization [74], we can determine the flow of electricity from generators to consumers in the power network. We used our FT/ET-based CCD library in HOL4 to analyze all possible safety classes of reliability and failure consequence events that can occur in the electrical power network at the distributed generation subsystem level. Subsequently, we determine accuracy of power system reliability indices, such as Forced Outage Rate (FOR) for all generation power plants and System Average Interruption Duration Index (SAIDI). Typically, we are only interested in evaluating the duration of certain failure events occurrence for specific loads in the grid. For instance, if we consider the failure of load A, which according to the OPF is supplied from G9 and G5 only, as shown in Figure 4.6, then the failure of either one or both power plants will lead to a partial or a complete blackout failure at that load, respectively. Assuming the failure of one power plant causes a load-shedding [80] of 25% of the connected load demand while two consecutive complete failures of PV/Steam generation power plants causes a blackout of the supplied load. Therefore, we can observe different levels of Complete Failure (CF) and Partial Failure (PF) for loads A, B, C and D (Figure4.6) in the power network as follows:

1. $Pr(\mathrm{A}_{PF}\lightning) = (1 - \mathrm{FOR}_{G_9}) \times \mathrm{FOR}_{G_5} + \mathrm{FOR}_{G_9} \times (1 - \mathrm{FOR}_{G_5})$

2. $Pr(\mathrm{A}_{CF}\lightning) = (1 - \mathrm{FOR}_{G_9}) \times (1 - \mathrm{FOR}_{G_5})$

3. $Pr(\mathrm{B}_{PF}\lightning) = (1 - \mathrm{FOR}_{G_9}) \times \mathrm{FOR}_{G_7} + \mathrm{FOR}_{G_9} \times (1 - \mathrm{FOR}_{G_7})$

4. $Pr(\mathrm{B}_{CF}\lightning) = (1 - \mathrm{FOR}_{G_9}) \times (1 - \mathrm{FOR}_{G_7})$

5. $Pr(\mathrm{C}_{PF}\lightning) = (1 - \mathrm{FOR}_{G_1}) \times \mathrm{FOR}_{G_2} + \mathrm{FOR}_{G_1} \times (1 - \mathrm{FOR}_{G_2})$

6. $Pr(\mathrm{C}_{CF}\lightning) = (1 - \mathrm{FOR}_{G_1}) \times (1 - \mathrm{FOR}_{G_2})$

7. $$\begin{aligned} Pr(\mathrm{D}_{PF}\lightning) = {} & (1 - \mathrm{FOR}_{G_6}) \times (1 - \mathrm{FOR}_{G_3}) \times (1 - \mathrm{FOR}_{G_8}) \times \mathrm{FOR}_{G_4} \\ & + (1 - \mathrm{FOR}_{G_6}) \times (1 - \mathrm{FOR}_{G_3}) \times \mathrm{FOR}_{G_8} \times (1 - \mathrm{FOR}_{G_4}) \\ & + \mathrm{FOR}_{G_6} \times (1 - \mathrm{FOR}_{G_3}) \times (1 - \mathrm{FOR}_{G_8}) \times (1 - \mathrm{FOR}_{G_4}) \end{aligned}$$

8. $$\begin{aligned} Pr(\mathrm{D}_{CF}\lightning) = {} & (1 - \mathrm{FOR}_{G_6}) \times (1 - \mathrm{FOR}_{G_3}) \times \mathrm{FOR}_{G_8} \times \mathrm{FOR}_{G_4} \\ & + (1 - \mathrm{FOR}_{G_6}) \times \mathrm{FOR}_{G_3} \times (1 - \mathrm{FOR}_{G_8}) \times \mathrm{FOR}_{G_4} \\ & + (1 - \mathrm{FOR}_{G_6}) \times \mathrm{FOR}_{G_3} \times \mathrm{FOR}_{G_8} \\ & + \mathrm{FOR}_{G_6} \times (1 - \mathrm{FOR}_{G_3}) \times (1 - \mathrm{FOR}_{G_8}) \times \mathrm{FOR}_{G_4} \\ & + \mathrm{FOR}_{G_6} \times \mathrm{FOR}_{G_3} \end{aligned}$$

Therefore, the assessment of SAIDI at the generation subsystem level (FOR) for the Electrical Power Network (EPN), can be written mathematically as follows:

$$\mathrm{SAIDI}_{EPN} = \frac{\begin{array}{l} Pr(\mathrm{A}_{CF}\lightning) \times \mathrm{MTTR}_{A} \times \mathrm{CN}_{A} + Pr(\mathrm{A}_{PF}\lightning) \times \mathrm{MTTR}_{A} \times 20\%\mathrm{CN}_{A} + \\ Pr(\mathrm{B}_{CF}\lightning) \times \mathrm{MTTR}_{B} \times \mathrm{CN}_{B} + Pr(\mathrm{B}_{PF}\lightning) \times \mathrm{MTTR}_{B} \times 20\%\mathrm{CN}_{B} + \\ Pr(\mathrm{C}_{CF}\lightning) \times \mathrm{MTTR}_{C} \times \mathrm{CN}_{C} + Pr(\mathrm{C}_{PF}\lightning) \times \mathrm{MTTR}_{C} \times 20\%\mathrm{CN}_{C} + \\ Pr(\mathrm{D}_{CF}\lightning) \times \mathrm{MTTR}_{A} \times \mathrm{CN}_{D} + Pr(\mathrm{D}_{PF}\lightning) \times \mathrm{MTTR}_{D} \times 20\%\mathrm{CN}_{D} \end{array}}{\mathrm{CN}_{A} + \mathrm{CN}_{B} + \mathrm{CN}_{C} + \mathrm{CN}_{D}} \tag{4.16}$$

In order to verify the above expressions for reliability indices at the subsystem level, in the next subsections, we first formalize the reliability and energy indices of Equations 3.1-3.10 based on CCD models, then formally model the IEEE 39-bus power network and verify its reliability with a discussion of experimental results.

4.3.1 Formal CCD Reliability and Energy Indices

We define a function $\mathtt{Prob}^{\mathtt{CCD}}_{\mathtt{X}}\lightning$ corresponding to the probability of failure $\lightning$ for location X based on the CCD analysis, then we define two functions $\sum^{\mathtt{Interrupt}}_{\mathtt{Load}}\lightning$ and $\sum^{\mathtt{Duration}}_{\mathtt{Load}}\lightning$ that provide the load customer interruptions and interruption durations, respectively, in HOL4 as follows:

Definition 4.12. *Probability of Location X Complete/Partial Failure*

$\vdash \mathtt{Prob}^{\mathtt{CCD}}_{\mathtt{X}}\lightning\ \mathtt{p}\ (\mathtt{Path}_1\mathtt{::Path}_{\mathcal{N}})\ \mathtt{=\ prob\ p}\ \big(\mathtt{CONSEQ\_BOX\ p}\ (\mathtt{Path}_1\mathtt{::Path}_{\mathcal{N}})\big)$

Definition 4.13. *Total Number of Load Customer Interruptions*

$\vdash \sum^{\mathtt{Interrupt}}_{\mathtt{Load}}\lightning\ \mathtt{p}\ (\mathtt{Path}_{\mathcal{N}}\mathtt{::Path}_{\mathcal{N}All})\ (\mathtt{CN::CN}_{\mathcal{N}})\ \mathtt{=}$

$\big(\mathtt{Prob}^{\mathtt{CCD}}_{\mathtt{X}}\lightning\ \mathtt{p}\ \mathtt{Path}_{\mathcal{N}}\big)\ \times\ \mathtt{CN}\ \mathtt{+}\ \sum^{\mathtt{Interrupt}}_{\mathtt{Load}}\lightning\ \mathtt{p}\ \mathtt{Path}_{\mathcal{N}All}\ \mathtt{CN}_{\mathcal{N}}$

where $\mathtt{Path}_{\mathcal{N}All}$ is a three-dimensional list of all power grid load CCD different failure paths under study, while $\mathtt{CN}_{\mathcal{N}}$ is the list of all customer numbers.

Definition 4.14. *Total Number of Load Customer Interruption Durations*

$$\vdash \textstyle\sum_{\texttt{Load}}^{\texttt{Duration}} \text{↯}\ \texttt{p}\ (\texttt{Path}_{\mathcal{N}}\texttt{::Path}_{\mathcal{N}All})\ (\texttt{MTTR::MTTR}_{\mathcal{N}})\ (\texttt{CN::CN}_{\mathcal{N}})\ \texttt{=}$$

$$\left(\texttt{Prob}_{\texttt{X}}^{\texttt{CCD}}\text{↯}\ \texttt{p Path}_{\mathcal{N}}\right)\ \times\ \texttt{MTTR}\ \times\ \texttt{CN}\ \texttt{+}\ \textstyle\sum_{\texttt{Load}}^{\texttt{Duration}} \text{↯}\ \texttt{p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}$$

where $\texttt{MTTR}_{\mathcal{N}}$ is the list of all MTTRs. Now, we define the `SAIFI` function as the total number of customer interruptions at the subsystem level over the total number of customers served as well as we define the `SAIDI` function as the sum of all customer interruption durations at the subsystem level over the total number of customers served. Similarly, we define the functions `CAIDI`, `ASAI`, `ASAI`, `ASUI`, as described in Equations 3.3-3.5 (Section 3.3.1) at the subsystem level, respectively, in HOL4 as:

`System Average Interruption Frequency Index (SAIFI):`

Definition 4.15. *SAIFI Reliability Index*

$$\vdash \texttt{SAIFI p Path}_{\mathcal{N}All}\ \texttt{CN}_{\mathcal{N}}\ \texttt{=}\ \frac{\sum_{\texttt{Load}}^{\texttt{Interrupt}} \text{↯}\ \texttt{p Path}_{\mathcal{N}All}\ \texttt{CN}_{\mathcal{N}}}{\sum \texttt{CN}_{\mathcal{N}}}$$

`System Average Interruption Duration Index (SAIDI):`

Definition 4.16. *SAIDI Reliability Index*

$$\vdash \texttt{SAIDI p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{=}\ \frac{\sum_{\texttt{Load}}^{\texttt{Duration}} \text{↯}\ \texttt{p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}}{\sum \texttt{CN}_{\mathcal{N}}}$$

`Customer Average Interruption Duration Index (CAIDI):`

Definition 4.17. *CAIDI Reliability Index*

$$\vdash \texttt{CAIDI p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{=}\ \frac{\texttt{SAIDI p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}}{\texttt{SAIFI p Path}_{\mathcal{N}All}\ \texttt{CN}_{\mathcal{N}}}$$

`Average Service Availability Index (ASAI):`

Definition 4.18. *ASAI Reliability Index*

$$\vdash \texttt{ASAI p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\texttt{=}$$

$$\frac{\sum \texttt{CN}_{\mathcal{N}} \times 8760 - \sum_{\texttt{Load}}^{\texttt{Duration}} \text{↯}\ \texttt{p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}}{\sum \texttt{CN}_{\mathcal{N}} \times 8760}$$

Average Service Unavailability Index (ASUI):

Definition 4.19. *ASUI Reliability Index*

$$\vdash \texttt{ASUI p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}} = \frac{\sum_{\texttt{Load}}^{\texttt{Duration}} \text{↯}\ \texttt{p Path}_{\mathcal{N}All}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}}{\sum \texttt{CN}_{\mathcal{N}} \times 8760}$$

We can also formally define the energy indices, i.e., `ENS`, `ASCI`, `LOLE`, `LOEE`, `EIR` as (see Equations 3.6-3.10), based on CCD analysis at the subsystem level, to ensure the delivery of electrical power without failures, respectively, in HOL4 as follows:

Energy not Supplied Index (ENS):

Definition 4.20. *ENS Reliability Index*

$$\vdash \texttt{ENS p (Path}_{\mathcal{N}}\texttt{::Path}_{\mathcal{N}All}\texttt{) (La::La}_{\mathcal{N}}\texttt{) (MTTR::MTTR}_{\mathcal{N}}\texttt{) =}$$

$$\texttt{La} \times \left(\texttt{Prob}_{\texttt{X}}^{\texttt{CCD}\text{↯}}\ \texttt{p Path}_{\mathcal{N}}\right) \times \texttt{MTTR + ENS p Path}_{\mathcal{N}All}\ \texttt{La}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}$$

where $\texttt{La}_{\mathcal{N}}$ is the list of all loads connected at all locations.

Average System Curtailment Index (ASCI):

Definition 4.21. *ASCI Reliability Index*

$$\vdash \texttt{ASCI p Path}_{\mathcal{N}All}\ \texttt{La}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}} = \frac{\texttt{ENS p Path}_{\mathcal{N}All}\ \texttt{La}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}}{\sum \texttt{CN}_{\mathcal{N}}}$$

Loss of Load Expectation (LOLE):

Definition 4.22. *LOLE Reliability Index*

$$\vdash \texttt{LOLE p (Path}_{\mathcal{N}}\texttt{::Path}_{\mathcal{N}All}\texttt{) (tk::tk}_{\mathcal{N}}\texttt{) =}$$

$$\left(\texttt{Prob}_{\texttt{X}}^{\texttt{CCD}\text{↯}}\ \texttt{p Path}_{\mathcal{N}}\right) \times \texttt{tk + LOLE p Path}_{\mathcal{N}All}\ \texttt{tk}_{\mathcal{N}}$$

where $\texttt{tk}_{\mathcal{N}}$ is the list of all days curtailed by the outages.

Loss of Energy Expectation (LOEE):

Definition 4.23. *LOEE Reliability Index*

$$\vdash \texttt{LOEE p (Path}_{\mathcal{N}}\texttt{::Path}_{\mathcal{N}All}\texttt{) (Ek::Ek}_{\mathcal{N}}\texttt{) =}$$

$$\left(\texttt{Prob}^{\texttt{CCD}}_{\texttt{X}}\lightning\ \texttt{p Path}_{\mathcal{N}}\right) \times \texttt{Ek + LOEE p Path}_{\mathcal{N}All}\ \texttt{Ek}_{\mathcal{N}}$$

where $\texttt{Ek}_{\mathcal{N}}$ is the list of all energy curtailed by the outages.

`Energy Index of Reliability (EIR):`

Definition 4.24. *EIR Reliability Index*

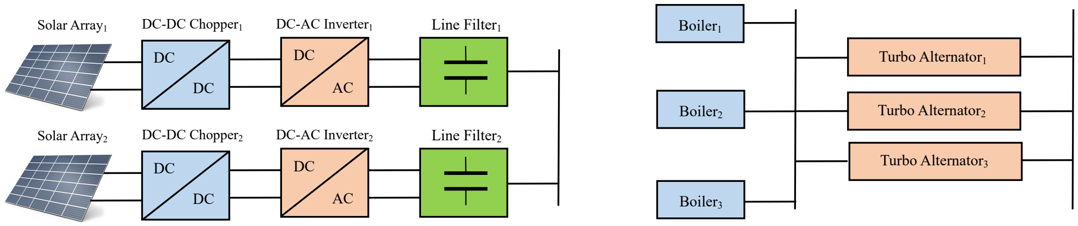
$$\vdash \texttt{EIR p Path}_{\mathcal{N}All}\ \texttt{Ek}_{\mathcal{N}}\ \texttt{E}_{T}\ \texttt{= 1 -}\ \frac{\texttt{LOEE p Path}_{\mathcal{N}All}\ \texttt{Ek}_{\mathcal{N}}}{\texttt{E}_{T}}$$

Now, we can apply our four steps of formal CCD analysis on the IEEE 39-bus generation power network shown in Figure 4.6 , in HOL4 as follows:

4.3.2 Formal CCD Model

Step 1 (Subsystem Failure Events):

Figure 4.7(a) and Figure 4.7(b) depict two typically realistic PV and steam generation power plants, respectively. The solar PV power plant consists of 2 solar farms connected in series configuration, where each farm is composed of four parts [60]: (i) a Solar Array (SA) generates a clean carbon-neutral power energy from the sun; (ii) a DC-DC converter or DC chopper controls the output DC voltage; (iii) a DC-AC Inverter converts the outcome DC voltage to the grid AC voltage; and lastly (iv) a Line Filter (LF) eliminates the undesired harmonics of voltage/current wave-forms. The steam power plant consists of 3 generators [83] connected in parallel configuration, where each generator is composed of two parts: (i) a Boiler or steam generator that creates steam flow by applying heat energy to water; and (ii) a Turbo Alternator (TA) steam turbine converts mechanical energy to electrical energy. Therefore, the FT model representing the PV power plant is constructed in OR configuration while the



(a) Solar PV Power Plant

(b) Steam Power Plant

Figure 4.7: Generation Power Plant Schematic Diagrams

FT model representing the steam power plant is constructed in AND configuration, as shown in Figure 4.8(a) and Figure 4.8(b), respectively. Using the formalization of FT in HOL4 (see Section 2.4), we can formally define the FT models of both PV and Steam plants, respectively, in HOL4 as follows:

Definition 4.25. *Fault Tree Model of Generator 1 Solar Power Plant*

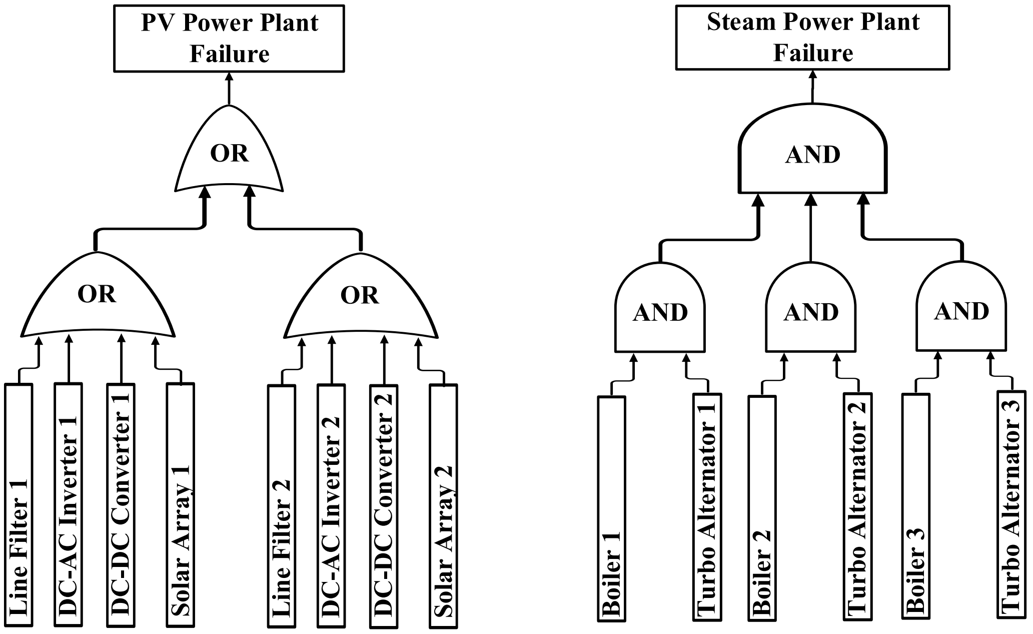
$\vdash$ FT_{PVG1} = FTree p (OR [OR [SA1G1 ↓;DC_DC1G1 ↓;DC_AC1G1 ↓;LF1G1 ↓];
OR [SA2G1 ↓;DC_DC2G1 ↓;DC_AC2G1 ↓;LF2G1 ↓]])

where the failure function ↓ assigns a continuous exponential failure probabilistic distribution to each component in the generation power plant to determine the probability of failure at a certain time t during the operation of the grid (see Section 2.4).

Definition 4.26. *Fault Tree Model of Generator 6 Steam Power Plant*

$\vdash$ $\mathrm{FT}_{STEAMG6}$ = FTree p (AND [AND [BO1G6 ↓;TA1G6 ↓];
AND [BO2G6 ↓;TA2G6 ↓];
AND [BO3G6 ↓;TA3G6 ↓]])

Also, we define the FT OR models of FT_{PVG2}, FT_{PVG3}, FT_{PVG4}, FT_{PVG5} corresponding, respectively, to the PV power plants G2-G5 similar to FT_{PVG1}. Moreover, we define the FT AND models of $\mathrm{FT}_{STEAMG7}$, $\mathrm{FT}_{STEAMG8}$, $\mathrm{FT}_{STEAMG9}$ corresponding, respectively, to the steam power plant G7-G9 similar to $\mathrm{FT}_{STEAMG6}$.



(a) FT Model of a PV Power Plant

(b) FT Model of a Steam Power Plant

Figure 4.8: Fault Tree Models of the Electrical Power Plants

Steps 2 and 3 (Construction of a CCD and Reduction):

We formally analyze up to *4-level* cause consequence reliability analysis of loads A, B, C and D at the subsystem-level for the electrical power network (Figure 4.6). We can reduce the number of test cases, as shown in Figure 4.9, by assigning an index number `X = 2` to all decision boxes required to be reduced from the generated complete CCD model (see Section 4.1). The reduced CCD model can be verified in HOL4 as follows:

Theorem 4.15. *Verification of Reduced CCD Model for Power Network Load A*

⊢ `Load_A_Reduced_CCD_Model` $\mathrm{FT}_{STEAMG9}$ FT_{PVG5} =

`CONSEQ_BOX p`

`[[DEC_BOX p 1 (`$\overline{\mathrm{FT}_{STEAMG9}}$`,`$\mathrm{FT}_{STEAMG9}$`);DEC_BOX p 1 (`$\overline{\mathrm{FT}_{PVG5}}$`,`$\mathrm{FT}_{PVG5}$`)];`

`[DEC_BOX p 1 (`$\overline{\mathrm{FT}_{STEAMG9}}$`,`$\mathrm{FT}_{STEAMG9}$`);DEC_BOX p 0 (`$\overline{\mathrm{FT}_{PVG5}}$`,`$\mathrm{FT}_{PVG5}$`)];`

`[DEC_BOX p 0 (`$\overline{\mathrm{FT}_{STEAMG9}}$`,`$\mathrm{FT}_{STEAMG9}$`);DEC_BOX p 1 (`$\overline{\mathrm{FT}_{PVG5}}$`,`$\mathrm{FT}_{PVG5}$`)];`

`[DEC_BOX p 0 (`$\overline{\mathrm{FT}_{STEAMG9}}$`,`$\mathrm{FT}_{STEAMG9}$`);DEC_BOX p 0 (`$\overline{\mathrm{FT}_{PVG5}}$`,`$\mathrm{FT}_{PVG5}$`)]]`

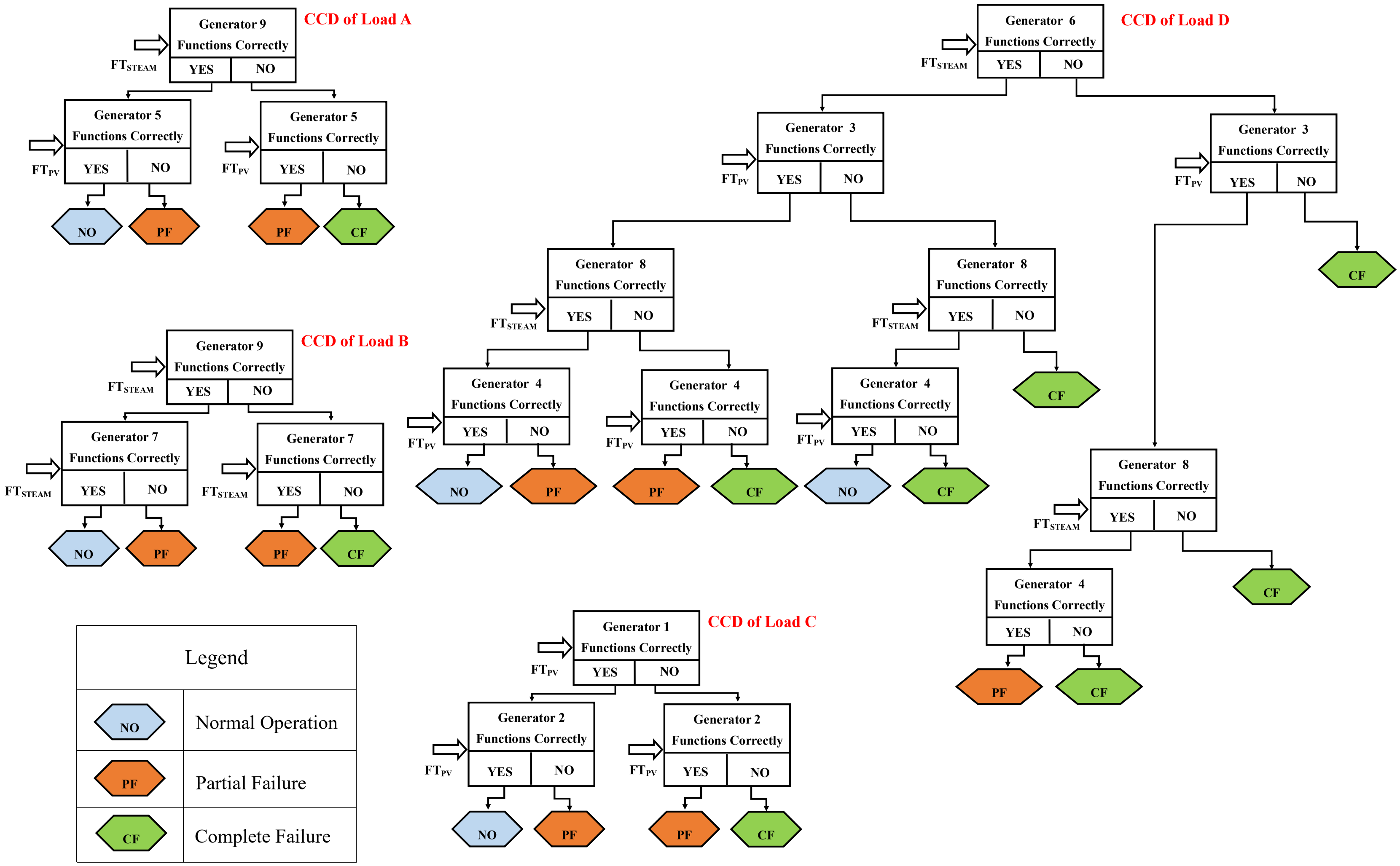

CCD of Load A
Generator 9 Functions Correctly
FT_{STEAM}
YES
NO
Generator 5 Functions Correctly
FT_{PV}
YES
NO
NO
PF
Generator 5 Functions Correctly
FT_{PV}
YES
NO
PF
CF
CCD of Load B
Generator 9 Functions Correctly
FT_{STEAM}
YES
NO
Generator 7 Functions Correctly
FT_{STEAM}
YES
NO
NO
PF
Generator 7 Functions Correctly
FT_{STEAM}
YES
NO
PF
CF
Legend
NO
Normal Operation
PF
Partial Failure
CF
Complete Failure
CCD of Load C
Generator 1 Functions Correctly
FT_{PV}
YES
NO
Generator 2 Functions Correctly
FT_{PV}
YES
NO
NO
PF
Generator 2 Functions Correctly
FT_{PV}
YES
NO
PF
CF
CCD of Load D
Generator 6 Functions Correctly
FT_{STEAM}
YES
NO
Generator 3 Functions Correctly
FT_{PV}
YES
NO
Generator 8 Functions Correctly
FT_{STEAM}
YES
NO
Generator 4 Functions Correctly
FT_{PV}
YES
NO
NO
PF
Generator 4 Functions Correctly
FT_{PV}
YES
NO
PF
CF
Generator 8 Functions Correctly
FT_{STEAM}
YES
NO
Generator 4 Functions Correctly
FT_{PV}
YES
NO
NO
CF
CF
Generator 3 Functions Correctly
FT_{PV}
YES
NO
CF
Generator 8 Functions Correctly
FT_{STEAM}
YES
NO
Generator 4 Functions Correctly
YES
NO
PF
CF
CF

Figure 4.9: Cause Consequence Analysis of Loads A, B, C and D for the IEEE 39-Bus Power Network

Theorem 4.16. *Verification of Reduced CCD Model for Power Network Load D*

$\vdash$ `Load_D_Reduced_CCD_Model` $\mathrm{FT}_{STEAMG6}$ FT_{PVG3} $\mathrm{FT}_{STEAMG8}$ FT_{PVG4} =

`CONSEQ_BOX p`

`[[DEC_BOX p 1` $(\overline{\mathrm{FT}_{STEAMG6}},\mathrm{FT}_{STEAMG6})$`;DEC_BOX p 1` $(\overline{\mathrm{FT}_{PVG3}},\mathrm{FT}_{PVG3})$`;`

`DEC_BOX p 1` $(\overline{\mathrm{FT}_{STEAMG8}},\mathrm{FT}_{STEAMG8})$`;DEC_BOX p 1` $(\overline{\mathrm{FT}_{PVG4}},\mathrm{FT}_{PVG4})$`];`

`[DEC_BOX p 1` $(\overline{\mathrm{FT}_{STEAMG6}},\mathrm{FT}_{STEAMG6})$`;DEC_BOX p 1` $(\overline{\mathrm{FT}_{PVG3}},\mathrm{FT}_{PVG3})$`;`

`DEC_BOX p 1` $(\overline{\mathrm{FT}_{STEAMG8}},\mathrm{FT}_{STEAMG8})$`;DEC_BOX p 0` $(\overline{\mathrm{FT}_{PVG4}},\mathrm{FT}_{PVG4})$`];`

$\vdots$

`[DEC_BOX p 0` $(\overline{\mathrm{FT}_{STEAMG6}},\mathrm{FT}_{STEAMG6})$`;DEC_BOX p 1` $(\overline{\mathrm{FT}_{PVG3}},\mathrm{FT}_{PVG3})$`;`

`DEC_BOX p 0` $(\overline{\mathrm{FT}_{STEAMG8}},\mathrm{FT}_{STEAMG8})$`];`

`[DEC_BOX p 0` $(\overline{\mathrm{FT}_{STEAMG6}},\mathrm{FT}_{STEAMG6})$`;DEC_BOX p 0` $(\overline{\mathrm{FT}_{PVG3}},\mathrm{FT}_{PVG3})$`]]`

4.3.3 Formal CCD Reliability Indices Assessment

The Force Outage Rate (FOR) of a power station unit is the probability that the unit will not be available for service when required while SAIDI is the sum of all interruption durations at each generation subsystem level over the total number of customers served.

`Force Outage Rate (FOR):`

Using Definitions FT_{PVG2}, FT_{PVG3}, FT_{PVG4}, FT_{PVG5}, FT_{PVG1}, $\mathrm{FT}_{STEAMG7}$, $\mathrm{FT}_{STEAMG8}$, $\mathrm{FT}_{STEAMG9}$, and $\mathrm{FT}_{STEAMG6}$, with the assumption that the failure states of generation power plant components are exponentially distributed, we can formally describe and verify the generated FOR expressions for all solar PV power plants G1-G5 and steam power plants G6-G9, for example, the FOR expressions of G1, G2 and G6, respectively, in HOL4 as follows:

Definition 4.27. *Force Outage Rate of Generator 1 Solar Power Plant*

$\vdash \mathrm{FOR}_{PVG1}$ `p = prob p` (FT_{PVG1})

Theorem 4.17. *Verification of FOR for Generator 1 Solar Power Plant*

$$\vdash \mathrm{FOR}_{PVG1}\ \texttt{p} = 1 - \mathrm{e}^{(-\lambda_{SA1G1}t)} \times \mathrm{e}^{(-\lambda_{DC\_DC1G1}t)} \times \mathrm{e}^{(-\lambda_{DC\_AC1G1}t)} \times \mathrm{e}^{(-\lambda_{LF1G1}t)} \times \mathrm{e}^{(-\lambda_{SA2G1}t)} \times \mathrm{e}^{(-\lambda_{DC\_DC2G1}t)} \times \mathrm{e}^{(-\lambda_{DC\_AC2G1}t)} \times \mathrm{e}^{(-\lambda_{LF2G1}t)}$$

Definition 4.28. *Force Outage Rate of Generator 2 Solar Power Plant*

$\vdash \mathrm{FOR}_{PVG2}$ `p = prob p` (FT_{PVG2})

Theorem 4.18. *Verification of FOR for Generator 2 Solar Power Plant*

$$\vdash \mathrm{FOR}_{PVG2}\ \texttt{p} = 1 - \mathrm{e}^{(-\lambda_{SA1G2}t)} \times \mathrm{e}^{(-\lambda_{DC\_DC1G2}t)} \times \mathrm{e}^{(-\lambda_{DC\_AC1G2}t)} \times \mathrm{e}^{(-\lambda_{LF1G2}t)} \times \mathrm{e}^{(-\lambda_{SA2G2}t)} \times \mathrm{e}^{(-\lambda_{DC\_DC2G2}t)} \times \mathrm{e}^{(-\lambda_{DC\_AC2G2}t)} \times \mathrm{e}^{(-\lambda_{LF2G2}t)}$$

Definition 4.29. *Force Outage Rate of Generator 6 Steam Power Plant*

$\vdash \mathrm{FOR}_{STEAMG6}$ `= prob p` $(\mathrm{FT}_{STEAMG6})$

Theorem 4.19. *Verification of FOR for Generator 6 Steam Power Plant*

$$\vdash \mathrm{FOR}_{STEAMG6}\ \texttt{p} = (1 - \mathrm{e}^{(-\lambda_{BO1G6}t)}) \times (1 - \mathrm{e}^{(-\lambda_{TA1G6}t)}) \times (1 - \mathrm{e}^{(-\lambda_{BO2G6}t)}) \times (1 - \mathrm{e}^{(-\lambda_{TA2G6}t)}) \times (1 - \mathrm{e}^{(-\lambda_{BO3G6}t)}) \times (1 - \mathrm{e}^{(-\lambda_{TA3G6}t)})$$

Similarly, we can generate FOR_{PVG3}, FOR_{PVG4}, FOR_{PVG5} corresponding to PV plants G3-G5 as well as $\mathrm{FOR}_{STEAMG7}$, $\mathrm{FOR}_{STEAMG8}$, $\mathrm{FOR}_{STEAMG9}$ corresponding to steam plants G7-G9 at the subsystem level.

`System Average Interruption Duration Index (SAIDI):`

Using Definition 4.16, we can formally verify the generated complex SAIDI_{EPN} expression at each generation PV and solar power plants subsystem level (Equation 4.16), in HOL4 as follows [84]:

Theorem 4.20. *Verification of Complex SAIDI at the Generation Level*

$\vdash$ `SAIDI =`

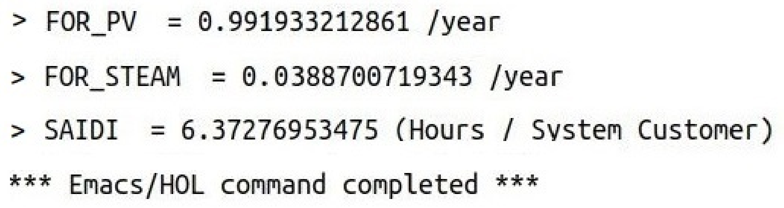
$$\frac{\begin{aligned}
&\Big(\big((1-\mathrm{e}^{(-\lambda_{BO1G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G9}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{BO3G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA3G9}t)})\big)\times\\
&\quad\big(1-\mathrm{e}^{(-\lambda_{SA1G5}t)}\times\mathrm{e}^{(-\lambda_{DC\_DC1G5}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{LF2G5}t)}\big)\Big)\times\mathrm{MTTR}_A\times\mathrm{CN}_A+\\
&\Big(\big(1-(1-\mathrm{e}^{(-\lambda_{BO1G9}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{BO3G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA3G9}t)})\big)\times\\
&\quad\big(1-\mathrm{e}^{(-\lambda_{SA1G5}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_AC2G5}t)}\times\mathrm{e}^{(-\lambda_{LF2G5}t)}\big)+\ldots\Big)\times\mathrm{MTTR}_A\times 15\%\ \ \mathrm{CN}_A+\\
&\Big(\big((1-\mathrm{e}^{(-\lambda_{BO1G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G9}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{BO3G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA3G9}t)})\big)\times\\
&\quad\big((1-\mathrm{e}^{(-\lambda_{BO1G7}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G7}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{TA3G7}t)})\big)\Big)\times\mathrm{MTTR}_B\times\mathrm{CN}_B+\\
&\Big(\big(1-(1-\mathrm{e}^{(-\lambda_{BO1G9}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G9}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{TA3G9}t)})\big)\times\\
&\quad\big((1-\mathrm{e}^{(-\lambda_{BO1G7}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{TA3G7}t)})\big)+\ldots\Big)\times\mathrm{MTTR}_B\times 15\%\ \ \mathrm{CN}_B+\\
&\Big(\big(1-\mathrm{e}^{(-\lambda_{SA1G1}t)}\times\mathrm{e}^{(-\lambda_{DC\_DC1G1}t)}\times\mathrm{e}^{(-\lambda_{DC\_AC1G1}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_AC2G1}t)}\times\mathrm{e}^{(-\lambda_{LF2G1}t)}\big)\times\\
&\quad\big(1-\mathrm{e}^{(-\lambda_{SA1G2}t)}\times\mathrm{e}^{(-\lambda_{DC\_DC1G2}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{LF2G2}t)}\big)\Big)\times\mathrm{MTTR}_C\times\mathrm{CN}_C+\\
&\Big(\big(\mathrm{e}^{(-\lambda_{SA1G1}t)}\times\mathrm{e}^{(-\lambda_{DC\_DC1G1}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_AC2G1}t)}\times\mathrm{e}^{(-\lambda_{LF2G1}t)}\big)\times\cdots\times\\
&\quad\big(\mathrm{e}^{(-\lambda_{SA1G3}t)}\times\mathrm{e}^{(-\lambda_{DC\_DC1G3}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_DC2G3}t)}\times\mathrm{e}^{(-\lambda_{DC\_AC2G3}t)}\times\mathrm{e}^{(-\lambda_{LF2G3}t)}\big)\times\\
&\quad\big((1-\mathrm{e}^{(-\lambda_{BO1G8}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G8}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{BO3G8}t)})\times(1-\mathrm{e}^{(-\lambda_{TA3G8}t)})\big)\times\\
&\quad\big(1-\mathrm{e}^{(-\lambda_{SA1G4}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_AC2G4}t)}\times\mathrm{e}^{(-\lambda_{LF2G4}t)}\big)+\ldots\Big)\times\mathrm{MTTR}_D\times\mathrm{CN}_D+\\
&\Big(\big(1-(1-\mathrm{e}^{(-\lambda_{BO1G6}t)})\times(1-\mathrm{e}^{(-\lambda_{TA1G6}t)})\times\cdots\times(1-\mathrm{e}^{(-\lambda_{TA3G6}t)})\big)\times\cdots\times\\
&\quad\big(1-\mathrm{e}^{(-\lambda_{SA1G4}t)}\times\cdots\times\mathrm{e}^{(-\lambda_{DC\_AC2G4}t)}\times\mathrm{e}^{(-\lambda_{LF2G4}t)}\big)+\ldots\Big)\times\mathrm{MTTR}_D\times 15\%\ \ \mathrm{CN}_D
\end{aligned}}{\mathrm{CN}_A+\mathrm{CN}_B+\mathrm{CN}_C+\mathrm{CN}_D}$$

The proof of the above complex expression of SAIDI at the subsystem-level helps power planners/designers to take critical decisions for power network improvements based on verified results. The proof of the above-verified SAIDI and SAIDI expressions at the subsystem level was conducted using HOL4 tactics, such as `DEP_REWRITE_TAC` and `EVAL_TAC` to apply our FT-based CCD probabilistic theorems on the goal and evaluate it, respectively. In the next section, we compare our formally obtained results with MATLAB MCS and also with *HiP-HOPS* [85] and FMR [86] for identifying and quantifying the failure modes for safety-critical systems at the subsystem level.

4.3.4 Numerical Results

We consider the failure rates of the power plant components λ_{BO}, λ_{TA}, λ_{LF}, $\lambda_{\text{DC\_DC}}$, $\lambda_{\text{DC\_AC}}$ and λ_{SA} are 0.91, 0.84, 0.96, 0.67, 0.22, and 0.56 per year, respectively [70]. Also, we assume that MTTR_A, MTTR_B, MTTR_C, and MTTR_D are 12, 20, 15, and 10 hours/interruption [69] and CN_A, CN_B, CN_C, and CN_D are 500, 1800, 900, and 2500 customers, respectively. The reliability study is undertaken for 1 year (365 days), i.e., $t = 8760$ hours. Based on the given data, we evaluate the FOR and SAIDI for the electrical power network in Figure 4.6 using the following four techniques:

1. ***HOL4 analysis*** using SML functions to evaluate FOR_{PV}, FOR_{STEAM}, and SAIDI in HOL4 (Theorems 4.17-4.20), respectively, as shown in Figure 4.10.



```
> FOR_PV  = 0.991933212861 /year
> FOR_STEAM  = 0.0388700719343 /year
> SAIDI  = 6.37276953475 (Hours / System Customer)
*** Emacs/HOL command completed ***
```

Figure 4.10: HOL4 Analysis: IEEE 39-Bus FOR and SAIDI Results

2. ***MATLAB MCS*** using a random-based algorithm to obtain different results of FOR and SAIDI in every run with a tolerance error between 4-9%. So, we present in Table 4.1 the best-estimated results of FOR and SAIDI with the least errors and then take the mean average of the obtained results.

Table 4.1: MATLAB MCS: IEEE 39-Bus FOR and SAIDI Results

MCS Simulated Run	FOR$_{PV}$ (G1-G5)	FOR$_{STEAM}$ (G6-G9)	SAIDI Reliability Index
1	88.55e-2	36.18e-3	5.8023
2	107.19e-2	40.03e-3	6.5045
3	93.52e-2	36.35e-3	6.0222
5	110.17e-2	43.03e-3	7.0495
4	95.24e-2	38.66e-3	6.3960
Average Result	98.93e-2	38.85e-3	6.3549

3. ***Failure Mode Reasoning (FMR)*** that mathematically identifies all failure modes of safety-critical system inputs that can result in an undesired state at its output. The FMR manual process consists of four main stages [87]: (a) *Composition*: Failure mode variables are defined and a set of logical implication statements is generated that express local failure modes; (b) *Substitution*: Local statements will be combined to create a single global implication statement between the critical-system inputs and outputs; (c) *Simplification*: The complex formula is simplified, where we trim off any redundant statements; and (d) *Calculation*: The probability of failure is evaluated using the failure rates. Based on the above-mentioned FMR procedures, we can express the component-level failure analysis of the PV power plant (Figure 4.8(a)) as follows:

$$(\hat{o} = \dot{f}) \Rightarrow (\hat{x}_1 = \dot{f} \vee \hat{x}_2 = \dot{f}) \tag{4.17}$$

The above equation means that if the output o is *False* caused by a fault then either one of its inputs to the OR gate, i.e., x_1 or x_2, must be *False* caused by a fault. We now need to determine what can cause $\hat{x}_1 = \dot{f}$ and $\hat{x}_2 = \dot{f}$. Similar to Equation 4.17, we can write:

$$(\hat{x_1} = \dot{f}) \Rightarrow (\hat{x_3} = \dot{f} \ \vee \hat{x_4} = \dot{f} \ \vee \hat{x_5} = \dot{f} \ \vee \hat{x_6} = \dot{f}) \tag{4.18}$$

$$(\hat{x_2} = \dot{f}) \Rightarrow (\hat{x_7} = \dot{f} \ \vee \hat{x_8} = \dot{f} \ \vee \hat{x_9} = \dot{f} \ \vee \hat{x_{10}} = \dot{f}) \tag{4.19}$$

where x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10} are LF_1, DC_DC_1, DC_AC_1, SA_1, LF_2, DC_DC_2, DC_AC_2, SA_2, respectively. Similarly, we can express the component-level failure analysis of the steam power plant (Figure 4.8(b)) as follows:

$$(\hat{o} = \dot{f}) \Rightarrow (\hat{x_{11}} = \dot{f} \ \wedge \hat{x_{12}} = \dot{f} \ \wedge \hat{x_{13}} = \dot{f}) \tag{4.20}$$

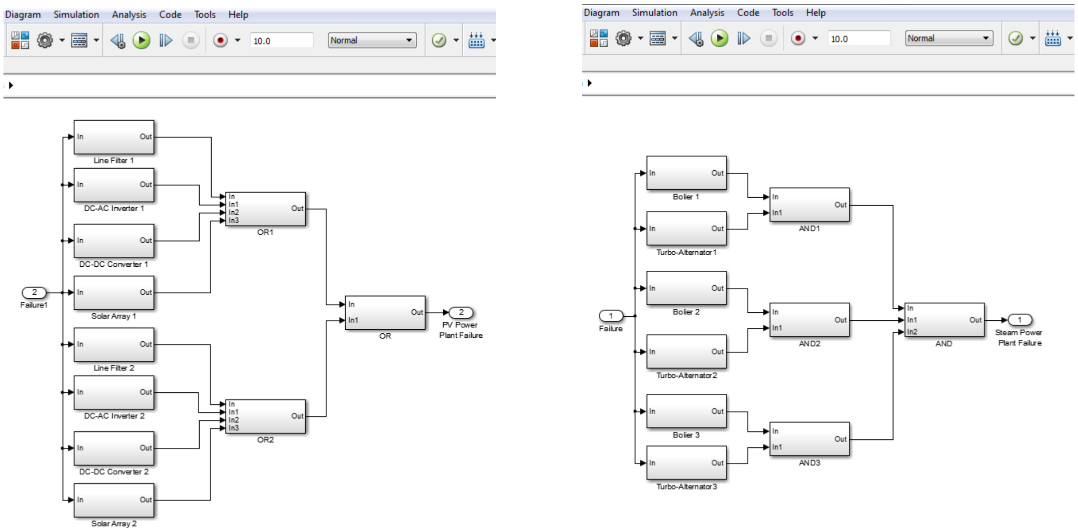
$$(\hat{x_{11}} = \dot{f}) \Rightarrow (\hat{x_{14}} = \dot{f} \ \wedge \hat{x_{15}} = \dot{f}) \tag{4.21}$$

$$(\hat{x_{12}} = \dot{f}) \Rightarrow (\hat{x_{16}} = \dot{f} \ \wedge \hat{x_{17}} = \dot{f}) \tag{4.22}$$

$$(\hat{x_{13}} = \dot{f}) \Rightarrow (\hat{x_{18}} = \dot{f} \ \wedge \hat{x_{19}} = \dot{f}) \tag{4.23}$$

where x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, are BO_1, TA_1, BO_2, TA_2, BO_3, TA_3, respectively. Table 4.2 shows the results of FOR$_{PV}$, FOR$_{STEAM}$, and SAIDI based on FMR analysis by substituting manually the component failure rates in Equation 4.17 to Equation 4.23. According to Jahanian et al. [86], the soundness of the obtained equations (Equation 4.17 to Equation 4.23) needs to be proven mathematically.

4. ***HiP-HOPS software*** that performs Failure Modes, Effects, and Critically Analyses (FMECA) [88] by building the architectural blocks that hierarchically describe a safety-critical system at the subsystem level. Figure 4.11(a) and Figure 4.11(b) depict the FMECA of the PV and steam power plants using the HiP-HOPS software, respectively. The probabilistic results of FOR$_{PV}$, FOR$_{STEAM}$, and SAIDI based on HiP-HOPS analysis are equivalent to the FMR analysis results presented in Table 4.2.



(a) HiP-HOPS: PV Plant FMECA

(b) HiP-HOPS: Steam Plant FMECA

Figure 4.11: IEEE 39-Bus FMECA Analysis using HIP-HOPS

It can be observed from Table 4.2 that FOR and SAIDI results at the subsystem level obtained from our formal HOL4 analysis are approximately equivalent to the corresponding ones calculated using FMR and HiP-HOPS approaches. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results of FOR and SAIDI every simulated run. The required time to model the 39-bus network using HiP-HOPS and FMR techniques was similar (a matter of hours) but more than the time for building the MATLAB algorithm. All three tools required more time than the modeling for the HOL4 analysis. This clearly demonstrates that

Table 4.2: Comparison of FOR and SAIDI Results

IEEE 39-Bus Reliability Indices	MATLAB	FMR	HiP-HOPS	HOL4
FOR_{PV} (/year)	98.93e-2	99.19e-2	99.19e-2	99.1933212861e-2
FOR_{STEAM} (/year)	38.85e-3	38.87e-3	38.87e-3	38.8700719343e-3
SAIDI (Hours/Customer)	6.3549	6.3728	6.3728	6.37276953475

our formal subsystem level reliability analysis is not only providing the correct result but also with a *formally proven* expressions (Theorems 4.17-4.20) compared to the other methods, i.e., the soundness of subsystem-level reliability analysis.

4.4 Summary

In this chapter, we conducted the formalization of FT-based cause consequence analysis. We formalized the CCD basic constructors, such as *Decision box*, *Consequence path* and *Consequence box*, that can be used to build an arbitrary level of CCDs. We enabled the formal reduction of CCDs that can remove unnecessary decision boxes from a given CCD model, a feature not available in other existing approaches. We provided reasoning support for formal probabilistic analysis of multi-level CCD consequence paths. We conducted the proofs in HOL4 using our developed ET theory (including the loading of all its parent theories) and the existing FT theory in HOL4. The proof-script of the FT-based CCD formalization work amounts to about 7000 lines of HOL4 code [84]. We conducted an application of a realistic IEEE 39-bus electrical power network system and provided the verification of its reliability indexes FOR and SAIDI at each generation subsystem level. The power system case study could seem simple but we are analyzing at the subsystem level which indicates complex reliability indexes expressions. A comparison with the corresponding results obtained from MATLAB MCS, FMR and HIP-HOPS shows the validation of our evaluated formal results. However, in order to identify potential areas of poor reliability, safety analysts often require a reliability model that is close to the hierarchical structure of the subsystem components. For that reason, we propose in the next chapter a novel approach to conduct a CCD reliability analysis based on RBDs rather than FTs.

Chapter 5

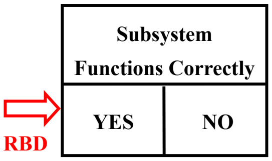
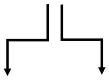
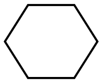
Formal RBD-based Cause Consequence Reliability Analysis

In this chapter, we introduce a novel idea of using RBD series and parallel configurations for the cause consequence reliability analysis of safety-critical systems. Then, we present the detailed formalization of RBD-based cause-consequence reliability analysis in HOL4, using a combination of the existing formalization of Reliability Block Diagrams (RBDs) in HOL4 (Section 2.4) and our formalization of Event Trees (ET) proposed in Chapter 3. We apply the developed RBD-based CCD analysis formalization on a smart power grid that consists of multiple interconnected Micro-Grids incorporating 100% green power plants.

5.1 RBD-Based CCD

Based on the observation that the components of many realistic systems are connected in parallel or series configurations, we realized that it would be much easier to model CCD diagrams using RBDs rather than FTs. Therefore, we propose to analyze all subsystems using RBD configurations. The proposed new CCD basic constructors *Decision box*, *Consequence path* and *Consequence box* are illustrated in Table 5.1. Figure 5.1 illustrates the corresponding RBD/ET-based cause consequence analysis, where different RBD configurations, such as *series* (models the complete success of the subsystem if all of the input success events occur at the same time) and *parallel* (models the complete success of the subsystem if any of the input success events occurs alone), are associated with all CCD decision boxes to model the reliability of a generic number of subsystems. As shown in Figure 5.1, the output of each YES BOX for all decision boxes is equal to the RBD outcome (RBD_X), while the NO BOX is the complement of the RBD model ($\overline{\text{RBD}_\text{X}}$), which is the opposite of cause consequence analysis based on FTs (see Figure 4.3).

Table 5.1: The Proposed New CCD Symbols and Functions

CCD Symbol	Function
	Decision Box: represents the status of functionality for a component or subsystem. (1) YES Box: describes the subsystem reliability operation. An RBD of the subsystem is connected to this box that can be used to obtain the reliability probability, i.e., $Pr_{\text{YES}} = Pr_{\text{RBD}}$ (2) NO Box: represents the not correct functioning of the subsystem or failure, which can be determined by simply taking the complement of the reliability operation, i.e., $Pr_{\text{NO}} = 1 - Pr_{\text{RBD}}$
	Consequence Path: models all possible consequence scenarios based on subsystem failure or reliability
	Consequence Box: models the final outcome due to a particular sequence of events for all subsystems

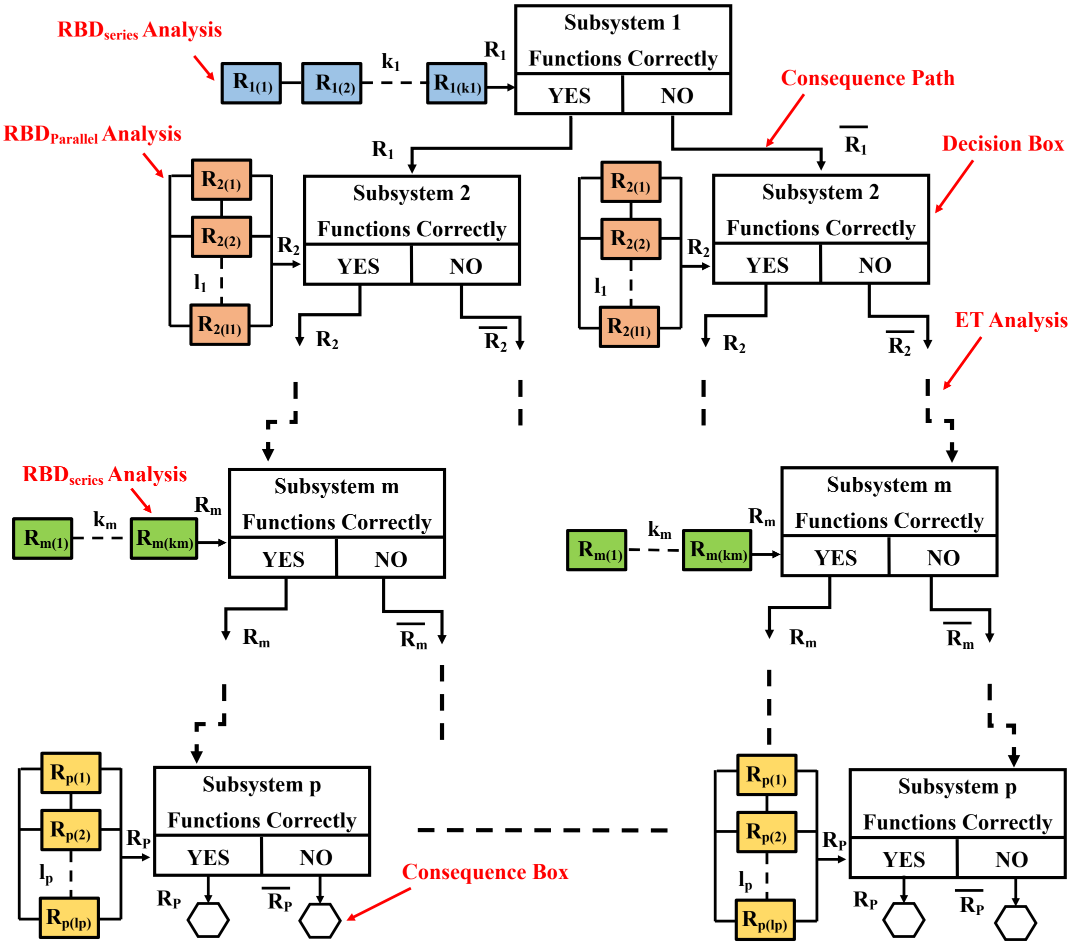


Figure 5.1: Proposed Multi-Level RBD/ET-based Cause Consequence Analysis

Example: Wind Turbine Generation System

To obtain a clear understanding of using RBDs instead of FTs in CCDs, consider a renewable carbon-neutral Wind Turbine (WT) generation system [89] in a Microgrid power network consisting of two main subsystems: Induction Generator (IG) and Power Converter (PC), as shown in Figure 5.2(a) [90]. An IG consists of three components *Stator*, *Rotor* and *Brushes* [91], while a PC consists of four components *Rotor Side AC/DC Converter* (RSC), *DC Filter*, *Grid Side DC/AC Converter* (GSC) and

Control Unit (CU) [92]. The four main steps of RBD/ET-based cause-consequence reliability analysis for the wind turbine system at the subsystem level can be done as:

1. *Components reliability events*: Assign an RBD series configuration to each subsystem in the wind turbine, i.e., $\mathcal{R}_{\text{IG}}$, $\mathcal{R}_{\text{PC}}$, as shown in Figure 5.2(b) [90], as:

$$\mathcal{R}_{\text{IG}} = \mathcal{R}_{\text{stator}} \times \mathcal{R}_{\text{rotor}} \times \mathcal{R}_{\text{brushes}} \tag{5.1}$$

$$\mathcal{R}_{\text{PC}} = \mathcal{R}_{\text{RSC}} \times \mathcal{R}_{\text{filter}} \times \mathcal{R}_{\text{GSC}} \times \mathcal{R}_{\text{CU}} \tag{5.2}$$

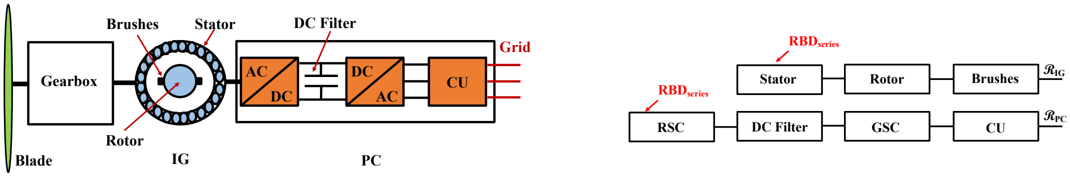
2. *Construction of a complete CCD*: Draw a complete CCD model of the wind turbine system, as shown in Figure 5.3(a).

3. *CCD model reduction*: Apply the reduction operation on the constructed complete CCD model, as shown in Figure 5.3(b).

4. *CCD probabilistic analysis*: The probabilistic assessment of the two consequence boxes WT_S and WT_F in Figure 5.3(b) can be expressed mathematically as:

$$\begin{aligned} &Pr(Consequence\_Box_{WT_S}) = Pr(\text{IG}_{\text{YES}}) \times Pr(\text{PC}_{\text{YES}}) \\ &= \mathcal{R}_{\text{stator}} \times \mathcal{R}_{\text{rotor}} \times \mathcal{R}_{\text{brushes}} \times \mathcal{R}_{\text{RSC}} \times \mathcal{R}_{\text{filter}} \times \mathcal{R}_{\text{GSC}} \times \mathcal{R}_{\text{CU}} \end{aligned} \tag{5.3}$$

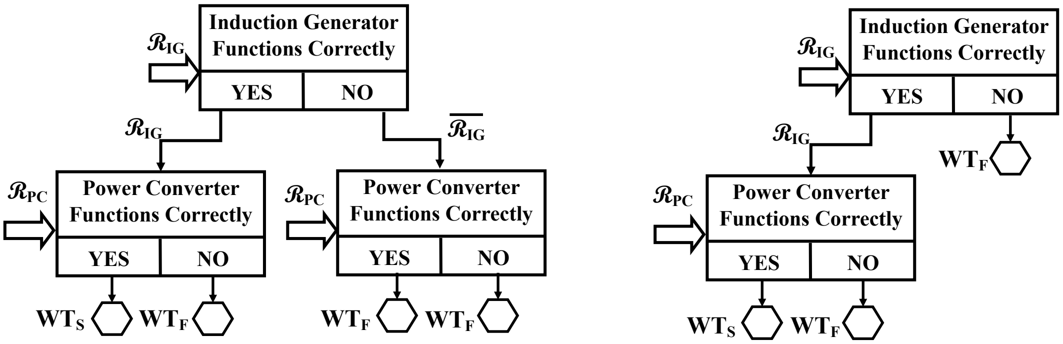
$$\begin{aligned} &Pr(Consequence\_Box_{WT_F}) = Pr(\text{IG}_{\text{YES}}) \times Pr(\text{PC}_{\text{NO}}) + Pr(\text{IG}_{\text{NO}}) \\ &= \mathcal{R}_{\text{stator}} \times \mathcal{R}_{\text{rotor}} \times \mathcal{R}_{\text{brushes}} \times (1 - \mathcal{R}_{\text{RSC}} \times \mathcal{R}_{\text{filter}} \times \mathcal{R}_{\text{GSC}} \times \mathcal{R}_{\text{CU}}) + \\ &(1 - \mathcal{R}_{\text{stator}} \times \mathcal{R}_{\text{rotor}} \times \mathcal{R}_{\text{brushes}}) \end{aligned} \tag{5.4}$$



(a) WT Structure

(b) RBD Models of WT Subsystems

Figure 5.2: Wind Turbine (WT) System


Induction Generator Functions Correctly
YES
NO
$\mathcal{R}_{IG}$
$\mathcal{R}_{IG}$
$\overline{\mathcal{R}_{IG}}$
Power Converter Functions Correctly
$\mathcal{R}_{PC}$
YES
NO
Power Converter Functions Correctly
$\mathcal{R}_{PC}$
YES
NO
WT_S
WT_F
WT_F
WT_F
Induction Generator Functions Correctly
$\mathcal{R}_{IG}$
YES
NO
$\mathcal{R}_{IG}$
WT_F
Power Converter Functions Correctly
$\mathcal{R}_{PC}$
YES
NO
WT_S
WT_F

(a) WT Complete CCD Model

(b) WT Reduced CCD Model

Figure 5.3: Wind Turbine Cause Consequence Analysis

5.2 Formal RBD-CCD Model

We can use the generic definitions of CCD basic constructors *Decision box*, *Consequence path* and *Consequence box*, as presented in Section 4.1 (i.e., Definitions 4.1, 4.2 and 4.3, respectively) to construct an RBD-based CCD model. For instance, we can formally construct a complete CCD model for the wind turbine shown in Figure 5.3(a), in HOL4 as follows:

Definition 5.1. *Complete CCD Model of the Wind Turbine System*

$\vdash$ Wind_Turbine_Complete_CCD_Model $\mathcal{R}_{\text{IG}}$ $\mathcal{R}_{\text{PC}}$ =

CONSEQ_BOX p [[DEC_BOX p 1 ($\mathcal{R}_{\text{IG}}$,$\overline{\mathcal{R}_{\text{IG}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{PC}}$,$\overline{\mathcal{R}_{\text{PC}}}$)];

[DEC_BOX p 1 ($\mathcal{R}_{\text{IG}}$,$\overline{\mathcal{R}_{\text{IG}}}$); DEC_BOX p 0 ($\mathcal{R}_{\text{PC}}$,$\overline{\mathcal{R}_{\text{PC}}}$)];

[DEC_BOX p 0 ($\mathcal{R}_{\text{IG}}$,$\overline{\mathcal{R}_{\text{IG}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{PC}}$,$\overline{\mathcal{R}_{\text{PC}}}$)];

[DEC_BOX p 0 ($\mathcal{R}_{\text{IG}}$,$\overline{\mathcal{R}_{\text{IG}}}$); DEC_BOX p 0 ($\mathcal{R}_{\text{PC}}$,$\overline{\mathcal{R}_{\text{PC}}}$)]]

Also, we can formally verify the reduced CCD model of the WT system (i.e., assign `X = 2` to irrelevance decision boxes) corresponding to Figure 5.3(b), in HOL4 as follows:

Theorem 5.1. *Verification of the Reduced CCD Model of the Wind Turbine*

$\vdash$ `Wind_Turbine_Reduced_CCD` $\mathcal{R}_{\text{IG}}$ $\mathcal{R}_{\text{PC}}$ `=`

`CONSEQ_BOX p [[DEC_BOX p 1 (`$\mathcal{R}_{\text{IG}}$`,`$\overline{\mathcal{R}_{\text{IG}}}$`); DEC_BOX p 1 (`$\mathcal{R}_{\text{PC}}$`,`$\overline{\mathcal{R}_{\text{PC}}}$`)];`

`[DEC_BOX p 1 (`$\mathcal{R}_{\text{IG}}$`,`$\overline{\mathcal{R}_{\text{IG}}}$`); DEC_BOX p 0 (`$\mathcal{R}_{\text{PC}}$`,`$\overline{\mathcal{R}_{\text{PC}}}$`)];`

`[DEC_BOX p 0 (`$\mathcal{R}_{\text{IG}}$`,`$\overline{\mathcal{R}_{\text{IG}}}$`)]]`

5.3 Formal RBD-Based CCD Analysis

First, we verify in HOL4 the one CCD decision box series and parallel theorems, then we propose a set of new probabilistic formulations for different types of *multi-level* RBD-based cause consequence analysis and their formalizations in HOL4.

One CCD Decision Box

Figure 5.4 depicts a single CCD decision box associated with either a series or a parallel RBD pattern. It can be observed that the `YES BOX` of the former CCD diagram with a series RBD model is the outcome of Equation 2.11 and its `NO BOX` is the complement of Equation 2.11. Similarly, the `YES BOX` of the later CCD diagram with a parallel RBD model is the outcome of Equation 2.12 and its `NO BOX` is the complement of Equation 2.12. The probability of a consequence path for each CCD decision box assigned with a generic RBD configurations, i.e., series of N events or parallel of M events, as shown in Figure 5.4, is verified respectively, using the existing RBD formalization in HOL4 (see Table 2.4 in Section 2.4), as follows:

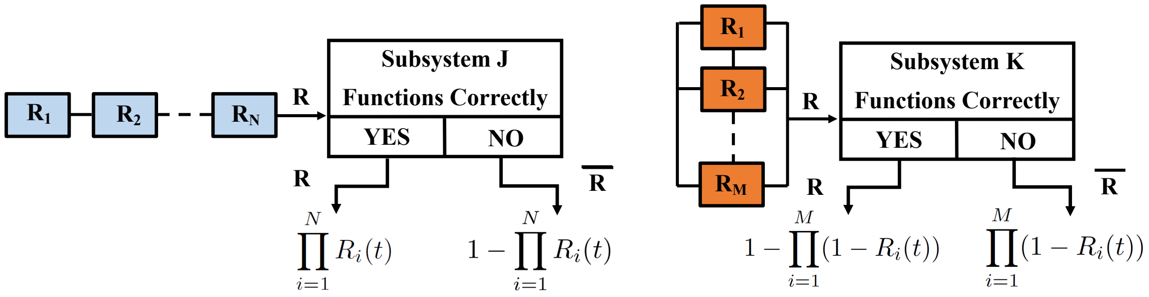


Figure 5.4: CCD Decision Boxes with RBD Connections

Theorem 5.2. *One Subsystem Decision Box of Series Configuration*

⊢ let $\text{RBD}_{\text{series}}$ = rbd_struct p (series R_N)
  in
  prob p
    (CONSEQ_PATH p
      [DEC_BOX p J ($\text{RBD}_{\text{series}}$,COMPL p ($\text{RBD}_{\text{series}}$))])
   = if J = 1 then $\prod$ (Pr_{L} p R_N)
  else if J = 0 then 1 - $\prod$ (Pr_{L} p R_N) else 1

Theorem 5.3. *One Subsystem Decision Box of Parallel Configuration*

⊢ let $\text{RBD}_{\text{parallel}}$ = rbd_struct p (parallel R_M)
  in
  prob p
    (CONSEQ_PATH p
      [DEC_BOX p K ($\text{RBD}_{\text{parallel}}$,COMPL p ($\text{RBD}_{\text{parallel}}$))])
   = if K = 1 then 1 - $\prod$ (Pr_{L} p (COMPL_LIST p R_M))
  else if K = 0 then $\prod$ (Pr_{L} p (COMPL_LIST p R_M)) else 1

where the function COMPL is defined to take the output of the RBD function R, and returns the complement of R in the probability space p. The function COMP_LIST takes a reliability list for components and returns the complement of the list reliability elements, i.e., $[(1-R_1),(1-R_2),\ldots,(1-R_n)]$ while $\mathrm{Pr_L}$ returns the probability list $[Pr(Z_1),Pr(Z_2),,\ \ldots,Pr(Z_{n-1}),Pr(Z_n)]$. The function $\prod$ returns the product of lists elements $X_1 \times X_2 \times X_3 \times X_4 \times \cdots \times X_{n-1} \times X_n$. For a complex graph of CCDs consisting of multi-level decision boxes, where each decision box is associated with a series/parallel RBD model consisting of an arbitrary list of success events, we define *three* types A, B and C with all possible consequence scenarios that can occur.

N CCD Decision Boxes of Type A

The probabilistic risk assessment of n decision boxes assigned to a consequence path corresponding to n subsystems of a complex system, where each decision box is associated with a generic RBD model consisting of a different arbitrary list of k events in a *series* connection, as shown in Figure 5.5(a), can be expressed mathematically for *three* cases as:

(A1) All outcomes of n decisions boxes are YES

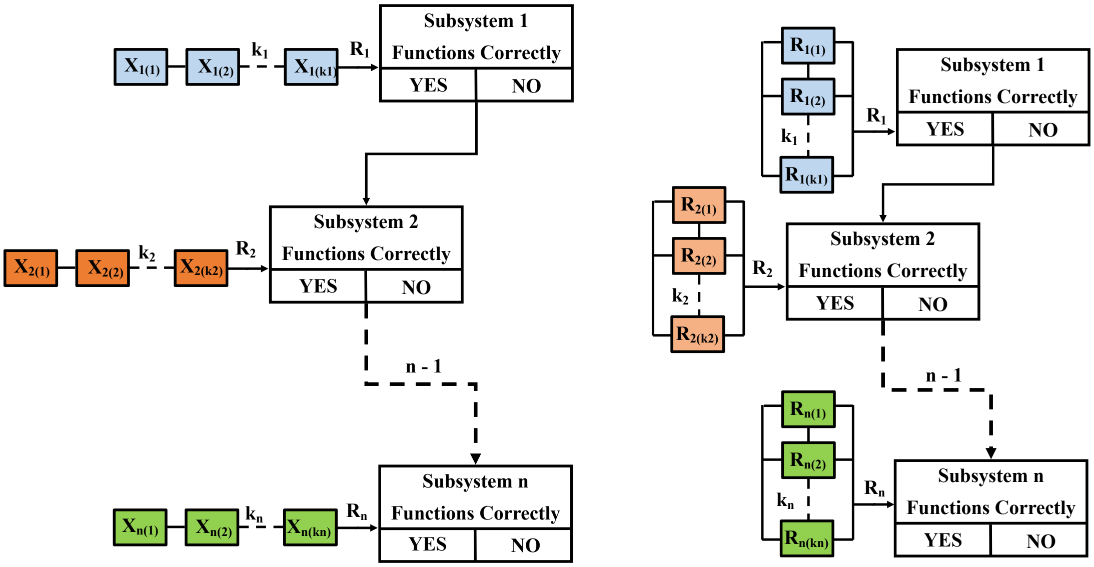
$$\mathcal{R}_{A1}(t) = \prod_{i=1}^{n}\prod_{j=1}^{k}\mathcal{R}_{ij}(t) \tag{5.5}$$

(A2) All outcomes of n decisions boxes are NO

$$\mathcal{R}_{A2}(t) = \prod_{i=1}^{n}(1-\prod_{j=1}^{k}\mathcal{R}_{ij}(t)) \tag{5.6}$$

(A3) Some outcomes of m out of n decisions boxes are YES and some outcomes of p out of n decisions boxes are NO

$$\mathcal{R}_{A3}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}(1-\prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \tag{5.7}$$



(a) Multi-level CCD Analysis of Type A (b) Multi-level CCD Analysis of Type B

Figure 5.5: Multi-level Decision Boxes for RBD/ET-based CCD Analysis

To formalize the above-proposed new cause-consequence mathematical formulations in HOL4, we formally define two functions $\mathcal{SS}^{YES}_{series}$ and $\mathcal{SS}^{NO}_{series}$ that can recursively generate the outcomes YES and NO of the RBD function `rbd_struct`, identified by RBD `series`, for a given arbitrary list of subsystems (SS) events, respectively as:

Definition 5.2. *Multi-Level Series Decision Boxes of YES Outcomes*

$\vdash$ $\mathcal{SS}^{YES}_{series}$ `p (SS1::SSN) =`

`rbd_struct p (series (rbd_list SS1))::`$\mathcal{SS}^{YES}_{series}$ `p SSN`

Definition 5.3. *Multi-Level Level Series Decision Boxes of NO Outcomes*

$\vdash$ $\mathcal{SS}^{NO}_{series}$ `p (SS1::SSN) =`

`COMPL p (rbd_struct p (series (rbd_list SS1)))::`$\mathcal{SS}^{NO}_{series}$ `p SSN`

Using the above defined functions, we can verify two-dimensional probabilistic formulations corresponding to Equations 5.5, 5.6 and 5.7, respectively, in HOL4 as:

Theorem 5.4. *Probability of Multi-Level Series Decision Boxes with All YES*

$\vdash$ `prob p` $\big($`CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{series}$ `p SSN)`$\big)$ `=`

$\prod$ `(MAP (`λ `a.` $\prod$ `(`$\mathrm{Pr_L}$ `p a)) SSN)`

Theorem 5.5. *Probability of Multi-Level Series Decision Boxes with All NO*

$\vdash$ `prob p` $\big($`CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{series}$ `p SSN)`$\big)$ `=`

$\prod$ `(MAP (`λ `b. (1 -` $\prod$ `(`$\mathrm{Pr_L}$ `p b))) SSN)`

Theorem 5.6. *Probability of Multi-Level Series Decision Boxes with NO/YES*

$\vdash$ `prob p`

$\big($`CONSEQ_PATH p`

`[CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{series}$ `p SSm); CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{series}$ `p SSp)]`$\big)$ `=`

$\Big($$\prod$ `(MAP (`λ `a.` $\prod$ `(`$\mathrm{Pr_L}$ `p a)) SSm)`$\Big)$ $\times$

$\Big($$\prod$ `(MAP (`λ `b. (1 -` $\prod$ `(`$\mathrm{Pr_L}$ `p b))) SSp)`$\Big)$

During the proof of Theorems 5.4-5.6, the verification was a bit challenging as we had to verify multiple *multi-level* lists connected simultaneously together, i.e., *multi-level* series decision boxes, *multi-level* complement of series decision boxes.

N CCD Decision Boxes of Type B

Similarly, the probabilistic risk assessment of n decision boxes assigned to a CCD path, where each decision box is associated with an RBD model consisting of different k events connected in *parallel*, can be expressed mathematically for *three* cases: (B1) All outcomes of n decisions boxes are YES; (B2) All outcomes of n decisions boxes are NO; and (B3) Some outcomes of m out of n decisions boxes are YES and some outcomes of p out of n decisions boxes are NO, as shown in Figure 5.5(b), respectively, as:

$$\mathcal{R}_{B1}(t) = \prod_{i=1}^{n}(1 - \prod_{j=1}^{k}(1 - \mathcal{R}_{ij}(t))) \tag{5.8}$$

$$\mathcal{R}_{B2}(t) = \prod_{i=1}^{n}\prod_{j=1}^{k}(1 - \mathcal{R}_{ij}(t)) \tag{5.9}$$

$$\mathcal{R}_{B3}(t) = \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}(1 - \mathcal{R}_{ij}(t)))\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{k}(1 - \mathcal{R}_{ij}(t))\right) \tag{5.10}$$

To verify the correctness of the above-proposed new CCD mathematical formulas in HOL4, we define two generic functions $\mathcal{SS}^{YES}_{parallel}$ and $\mathcal{SS}^{NO}_{parallel}$ to recursively generate the outcomes YES and NO of the function `rbd_struct`, identified by the RBD constructor `parallel`, for a given list of subsystems events.

Definition 5.4. *Multi-Level Parallel Decision Boxes of YES Outcomes*

⊢ $\mathcal{SS}^{YES}_{parallel}$ `p (SS1::SSN) =`

`rbd_struct p (parallel (rbd_list SS1))::`$\mathcal{SS}^{YES}_{parallel}$ `p SSN`

Definition 5.5. *Multi-Level Parallel Decision Boxes of NO Outcomes*

⊢ $\mathcal{SS}^{NO}_{parallel}$ `p (SS1::SSN) =`

`COMPL p (rbd_struct p (parallel (rbd_list SS1)))::`$\mathcal{SS}^{NO}_{parallel}$ `p SSN`

Using above functions, we can formally verify three two-dimensional probabilistic formulations corresponding to Equations 5.8, 5.9 and 5.10, respectively, in HOL4 as:

Theorem 5.7. *Probability of Multi-Level Parallel Decision Boxes with All YES*

⊢ `prob p` $\big($`CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{parallel}$ `p SSN)`$\big)$ `=`

$\prod$ `(MAP (`λ `a.  (1 -` $\prod$ `(`$\mathrm{Pr_L}$ `p (compl_list p a)))) SSN)`

Theorem 5.8. *Probability of Multi-Level Parallel Decision Boxes with All NO*

⊢ `prob p` $\big($`CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{parallel}$ `p SSN)`$\big)$ `=`

$\prod$ `(MAP (`λ `b.` $\prod$ `(`$\mathrm{Pr_L}$ `p (compl_list p b))) SSN)`

Theorem 5.9. *Probability of Multi-Level Parallel Decision Boxes with NO/YES*

$\vdash$ `prob p`

$\big($`CONSEQ_PATH p`

`[CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{parallel}$` p SSm); CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{parallel}$` p SSp)]`$\big)$ `=`

$\Big(\prod$ `(MAP (`λ `a.  (1 -` $\prod$ `(`$\mathrm{Pr_L}$ `p (compl_list p a)))) SSm)`$\Big) \times$

$\Big(\prod$ `(MAP (`λ `b.` $\prod$ `(`$\mathrm{Pr_L}$ `p (compl_list p b))) SSp)`$\Big)$

N CCD Decision Boxes of Type C

The probabilistic assessment of multi-level decision boxes assigned to a consequence path for a complex system, where some m decision boxes are associated with RBD models consisting of different k events connected in *series*, while other p decision boxes are associated with RBD models consisting of different l events connected in *parallel*, as shown in Figure 5.1, can be expressed mathematically for *nine* cases as:

(C1) All outcomes of m and p decisions boxes are YES.

$$\mathcal{R}_{C1}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}(1 - \prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t)))\right) \tag{5.11}$$

(C2) All outcomes of m and p decisions boxes are NO.

$$\mathcal{R}_{C2}(t) = \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t))\right) \tag{5.12}$$

(C3) All outcomes of m decisions boxes are YES and all outcomes of p decisions boxes are NO.

$$\mathcal{R}_{C3}(t) = \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t))\right) \tag{5.13}$$

(C4) All outcomes of m decisions boxes are NO and all outcomes of p decisions boxes are YES.

$$\mathcal{R}_{C4}(t) = \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{p}(1 - \prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t)))\right) \tag{5.14}$$

(C5) Some outcomes of s out of m decisions boxes are YES, some outcomes of u out of m decisions boxes are NO and all outcomes of p decisions boxes are YES.

$$\mathcal{R}_{C5}(t) = \left(\prod_{i=1}^{s}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \times \left(\prod_{i=1}^{u}(1 - \prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{p}(1 - \prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t)))\right) \tag{5.15}$$

(C6) Some outcomes of s out of m decisions boxes are YES, some outcomes of u out of m decisions boxes are NO and all outcomes of p decisions boxes are NO.

$$\mathcal{R}_{C6}(t) = \left(\prod_{i=1}^{s}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \times \left(\prod_{i=1}^{u}(1 - \prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{p}\prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t))\right) \tag{5.16}$$

(C7) Some outcomes of v out of p decisions boxes are YES, some outcomes of w out of p decisions boxes are NO and all outcomes of m decisions boxes are YES.

$$\mathcal{R}_{C7}(t) = \left(\prod_{i=1}^{v}(1 - \prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t)))\right) \times \left(\prod_{i=1}^{w}\prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{m}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right) \tag{5.17}$$

(C8) Some outcomes of v out of p decisions boxes are YES, some outcomes of w out of p decisions boxes are NO and all outcomes of m decisions boxes are NO.

$$\mathcal{R}_{C8}(t) = \left(\prod_{i=1}^{v}(1 - \prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t)))\right) \times \left(\prod_{i=1}^{w}\prod_{j=1}^{l}(1 - \mathcal{R}_{ij}(t))\right) \times \left(\prod_{i=1}^{m}(1 - \prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right) \tag{5.18}$$

Using Theorems 5.4-5.9, we formally verify in HOL4 all above formulas from Equation 5.11 to Equation 5.18 for RBD/ET-based cause consequence safety analysis, which is evidence for the correctness of the proposed formulations [93].

(C9) Some outcomes of s out of m decisions boxes are YES, some outcomes of u out of m decisions boxes are NO, some outcomes of v out of p decisions boxes are YES and some outcomes of w out of p decisions boxes are NO.

$$\begin{aligned}\mathcal{R}_{C9}(t) =& \left(\prod_{i=1}^{s}\prod_{j=1}^{k}\mathcal{R}_{ij}(t)\right)\times \\ & \left(\prod_{i=1}^{u}(1-\prod_{j=1}^{k}\mathcal{R}_{ij}(t))\right)\times \\ & \left(\prod_{i=1}^{v}(1-\prod_{j=1}^{l}(1-\mathcal{R}_{ij}(t)))\right)\times \\ & \left(\prod_{i=1}^{w}\prod_{j=1}^{l}(1-\mathcal{R}_{ij}(t))\right)\end{aligned} \tag{5.19}$$

Theorem 5.10. *Multi-Level Series/Parallel Decision Boxes with NO/YES*

$\vdash$ `prob p`

$\Big($`CONSEQ_PATH p`

`[CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{series}$` p SSs); CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{series}$` p SSu);`

`CONSEQ_PATH p (`$\mathcal{SS}^{YES}_{parallel}$` p SSv); CONSEQ_PATH p (`$\mathcal{SS}^{NO}_{parallel}$` p SSw)]`$\Big)$ `=`

$\Big(\prod$ `(MAP (`λ` a. ` $\prod$ `(`$\mathrm{Pr_L}$` p a)) SSs)`$\Big)$ $\times$

$\Big(\prod$ `(MAP (`λ` b. 1 - ` $\prod$ `(`$\mathrm{Pr_L}$` p b)) SSu)`$\Big)$ $\times$

$\Big(\prod$ `(MAP (`λ` c. (1 - ` $\prod$ `(`$\mathrm{Pr_L}$` p (compl_list p c)))) SSv)`$\Big)$ $\times$

$\Big(\prod$ `(MAP (`λ` d. ` $\prod$ `(`$\mathrm{Pr_L}$` p (compl_list p d))) SSw)`$\Big)$

The verification of all above complex theorem 5.10 was a bit challenging as we are dealing with all four types of different RBD configurations, i.e., series, the complement of series, parallel, and the complement of parallel, where each type is consisting of generic n-decision boxes and each decision box is associated with generic m-events, simultaneously in HOL4. Therefore, it was overwhelming to perform multi-level induction processes using the generic list theory during the proof of each probabilistic theorem. Remark that both FT/ET-based and RBD/ET-based cause consequence formalizations are not interchangeable as FT and RBD model reverse concepts of success and failure, respectively. Lastly, can use the same generic probabilistic formulation of a CCD `CONSEQ_BOX` (Theorem 4.14) for a certain event occurrence in the given system to sum of all individual probabilities of all $\mathcal{M}$ CCD consequence paths ending with a particular event. Moreover, we can use the same reliability and energy formulations for RBD/ET-based CCD analysis of critical systems (see Section 4.3.1).

To illustrate the applicability of our proposed approach, in the next section, we present the formal RBD-based cause consequence analysis of multiple interconnected Microgrids incorporating 100% RES as well as verify all reliability and energy indices at the generation subsystem level to ensure the delivery of power without failures.

5.4 Application: Interconnected Micro-Grids

Consider a realistic smart power grid consisting of four interconnected renewable and green Micro-Grids (MG) [94] incorporating 100% Renewable Energy Resources (RES) distributed green generation power plants, as shown in Figure 5.6 [69]. The MGs are designed to supply power to their local grids for an *island-mode* operation [95] as well as export/import power to/from the centralized power grid (Macrogrid) [96] on prior contract agreements. We use two main types of truly carbon-neutral or emissions-free green power generation [82] in the smart power grid (see Figure 5.6): (i) Wind-Turbine (WT) generating units of rated power 2,000 KW/WT [89]; and (ii) solar Photo-Voltaic (PV) generating units of rated power 1500 KW/PV [97]. Assuming that each WT power plant is consisting of five generating units connected in

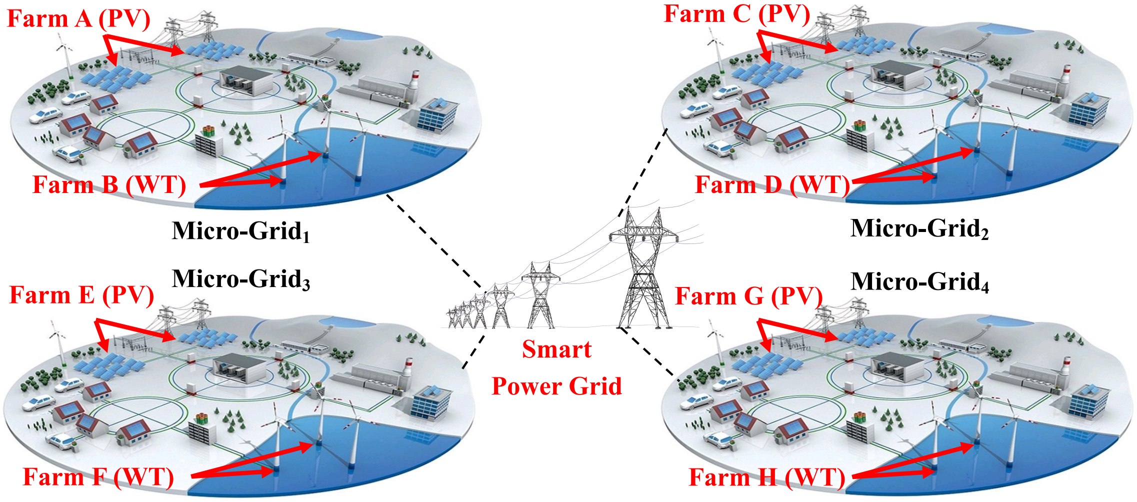


Figure 5.6: Interconnected Micro-Grids 100% RES of a Smart Power Grid

parallel configuration, i.e., Farm$_B$, Farm$_D$, Farm$_F$, Farm$_H$, while each PV power plant is consisting of five generating units connected in series configuration, i.e., Farm$_A$, Farm$_C$, Farm$_E$, Farm$_G$ to supply customers numbers CN$_{MG1}$, CN$_{MG2}$, CN$_{MG3}$, CN$_{MG4}$ within $Micro\ Grid_1$, $Micro\ Grid_2$, $Micro\ Grid_3$, $Micro\ Grid_4$, respectively [98]. The improvement of MGs reliability might be motivated by government regulation or by market competition [99], but it has become a significant subject in the power sector for both utilities and customers due to sudden increases in demand for a reliable MG power system at minimal frequency and duration of power outages [100].

5.4.1 Formal CCD Model

We use our RBD-based CCD formalization to perform the step-wise cause consequence analysis of the smart power grid shown in Figure5.6, namely, subsystem reliability events, construction of a complete CCD, CCD reduction, CCD probabilistic analysis.

Step 1 (Subsystem reliability events):

We formally define the RBD models of each WT and PV farm for all interconnected

MG power systems under the reliability study at the subsystem level, which are connected in parallel and series configurations as well as assign a reliability distribution or success function $\uparrow$ (Definition 2.2) to each WT and PV unit, in HOL4 as:

Definition 5.6. *RBD Model of Micro-Grid 1 Photo-Voltaic Farm A*

$\vdash \mathcal{R}_{\text{PVA}}$ =

```
  rbd_struct p (series [PV_A1 ↑,PV_A2 ↑,PV_A3 ↑,PV_A4 ↑,PV_A5 ↑])
```

Definition 5.7. *RBD Model of Micro-Grid 1 Wind Turbine Farm B*

$\vdash \mathcal{R}_{\text{WTB}}$ =

```
  rbd_struct p (parallel [WT_B1 ↑,WT_B2 ↑,WT_B3 ↑,WT_B4 ↑,WT_B5 ↑])
```

Similarly, we define $\mathcal{R}_{\text{PVC}}$, $\mathcal{R}_{\text{WTD}}$, $\mathcal{R}_{\text{PVE}}$, $\mathcal{R}_{\text{WTF}}$, $\mathcal{R}_{\text{PVG}}$, $\mathcal{R}_{\text{WTH}}$ corresponding to Farm C, Farm D, Farm E, Farm F, Farm G, Farm H, respectively [93].

Steps 2 and 3 (Construction of a CCD diagram):

We conduct an *8-level* cause consequence formal reliability analysis at the subsystem-level of all interconnected MGs (each MG consisting of 2 farms and each farm composed of 5 generating PV/WT units) simultaneously with a total of 256 possible scenarios. Assuming the failure of complete farm units at any of MG power systems causes a complete shutdown to that MG (load shedding) and thereupon the utility can maintain the frequency stability of the rest of the smart power grid [80] and prevent it to be subject to an undesirable blackout. Accordingly, the complete CCD model of the interconnected MGs can be reduced to 81 test cases, as shown in Figure 5.7, by assigning an index number `X =2` to all decision boxes required to be reduced from the generated complete CCD model. The reduced CCD model can be verified in HOL4 as:

Theorem 5.11. *Verification of Smart Power Grid Reduced CCD Model*

$$\begin{array}{l}
\vdash \texttt{Smart\_Power\_Grid\_Reduced\_CCD} \\
\qquad\qquad \mathcal{R}_{\mathrm{PVA}}\ \mathcal{R}_{\mathrm{WTB}}\ \mathcal{R}_{\mathrm{PVC}}\ \mathcal{R}_{\mathrm{WTD}}\ \mathcal{R}_{\mathrm{PVE}}\ \mathcal{R}_{\mathrm{WTF}}\ \mathcal{R}_{\mathrm{PVG}}\ \mathcal{R}_{\mathrm{WTH}} \\
\quad \texttt{= CONSEQ\_BOX p} \\
\qquad \texttt{[[DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVA}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVA}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{WTB}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTB}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVC}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVC}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{WTD}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTD}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVE}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVE}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{WTF}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTF}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVG}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVG}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{WTH}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTH}}}\texttt{)];} \\
\qquad \texttt{[DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVA}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVA}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{WTB}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTB}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVC}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVC}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{WTD}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTD}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 1 (}\mathcal{R}_{\mathrm{PVE}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVE}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{WTF}}\texttt{,}\overline{\mathcal{R}_{\mathrm{WTF}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{PVG}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVG}}}\texttt{)];} \\
\qquad\qquad\qquad \vdots \\
\qquad \texttt{[DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{PVA}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVA}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{PVC}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVC}}}\texttt{);} \\
\qquad\quad \texttt{DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{PVE}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVE}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\mathrm{PVG}}\texttt{,}\overline{\mathcal{R}_{\mathrm{PVG}}}\texttt{)]]}
\end{array}$$

It is worth to mention that the above reduced CCD model for analyzing the interconnected MGs at each generation level is exactly equivalent to the graphical CCD diagram in Figure 5.7. Moreover, based on the above-verified mathematical CCD model, we can evaluate sound and accurate energy indices, as described in the next section.

5.4.2 Formal CCD Energy Indices Assessment

Using our new generic probabilistic formulations (see Section 5.3), we can formally verify the probabilistic expression at the subsystem-level for any of the smart grid Capacity Outage Probability Table (COPT) [101], i.e., 0 MW (complete success), 17.5 MW, 35 MW, 52.5 MW and 70 MW (complete blackout), where each MG shown

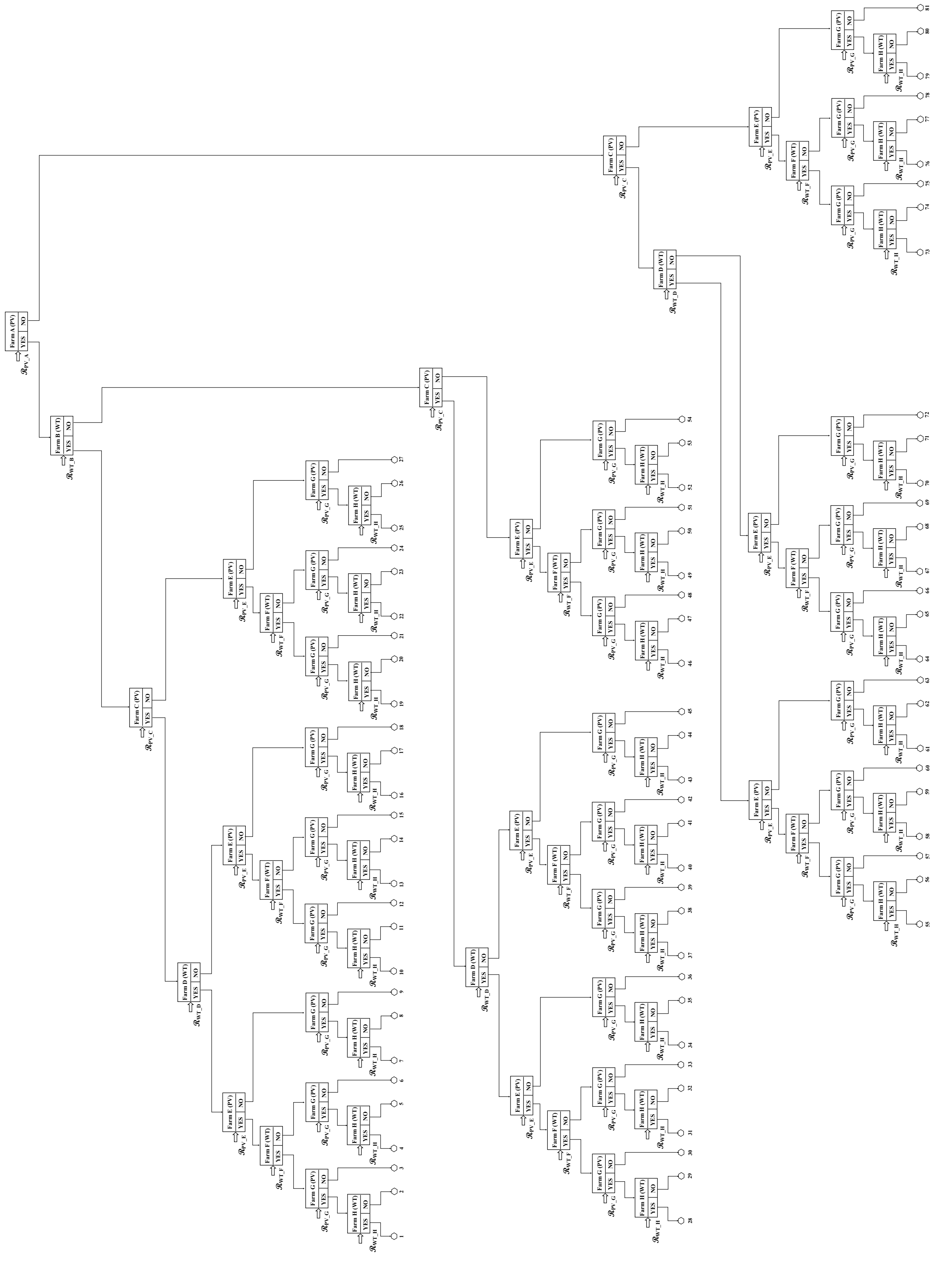


Figure 5.7: Cause Consequence Analysis of Interconnected Micro-Grids for the Smart Power Grid

in Figure 5.6 has a rated generation capacity of 17.5 MW (WT farm 2,000 × 5 KW and PV farm 1,500 × 5 KW). We assume that the PV/WT units of all MG power systems are continuous exponentially distributed [102] (see Section 2.4). We can observe the different behaviors of the smart power grid shown in Figure 5.7 as follows:

1. $\text{COPT}_{0MW} \quad = Pr_{(\text{Path}_1)}$
2. $\text{COPT}_{17.5MW} = \sum Pr_{\text{Paths}}\ (2, 3, 4, 7, 10, 19, 28, 55)$
3. $\text{COPT}_{35MW} \quad = \sum Pr_{\text{Paths}}\ (5, 6, 8, 9, 11, 12, 13, 16, 20, \ldots, 56, 57, 58, 61, 64, 73)$
4. $\text{COPT}_{52.5MW} = \sum Pr_{\text{Paths}}\ (14, 15, 17, 18, 23, 24, 26, \ldots, 66, 67, 70, 74, 75, 76, 79)$
5. $\text{COPT}_{70MW} \quad = \sum Pr_{\text{Paths}}(41, 42, 44, 45, 50, 51, 53, 54, 68, 69, 71, 72, 77, 78, 80, 81)$

For example, we can describe the COPT of the smart power grid from the generated reduced CCD model `Smart_Power_Grid_Reduced_CCD` and verify all its automatically generated probabilistic failure/reliability expressions at each MG subsystem level using Definition 4.12, e.g., COPT of 17.5 MW and 35 MW, respectively, in HOL4 as:

Definition 5.8. *Capacity Outage 17.5 MW*

⊢ COPT_17_5_MW $\mathcal{R}_{\text{PVA}}$ $\mathcal{R}_{\text{WTB}}$ $\mathcal{R}_{\text{PVC}}$ $\mathcal{R}_{\mathcal{WTD}}$ $\mathcal{R}_{\text{PVE}}$ $\mathcal{R}_{\text{WTF}}$ $\mathcal{R}_{\text{PVG}}$ $\mathcal{R}_{\text{WTH}}$ p =

$\text{Prob}_X^{CCD}\lightning$ p

[[DEC_BOX p 1 ($\mathcal{R}_{\text{PVA}}$,$\overline{\mathcal{R}_{\text{PVA}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{WTB}}$,$\overline{\mathcal{R}_{\text{WTB}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{PVC}}$,$\overline{\mathcal{R}_{\text{PVC}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{WTD}}$,$\overline{\mathcal{R}_{\text{WTD}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{PVE}}$,$\overline{\mathcal{R}_{\text{PVE}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{WTF}}$,$\overline{\mathcal{R}_{\text{WTF}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{PVG}}$,$\overline{\mathcal{R}_{\text{PVG}}}$); DEC_BOX p 0 ($\mathcal{R}_{\text{WTH}}$,$\overline{\mathcal{R}_{\text{WTH}}}$)];

$\vdots$

[DEC_BOX p 0 ($\mathcal{R}_{\text{PVA}}$,$\overline{\mathcal{R}_{\text{PVA}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{PVC}}$,$\overline{\mathcal{R}_{\text{PVC}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{WTD}}$,$\overline{\mathcal{R}_{\text{WTD}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{PVE}}$,$\overline{\mathcal{R}_{\text{PVE}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{WTF}}$,$\overline{\mathcal{R}_{\text{WTF}}}$); DEC_BOX p 1 ($\mathcal{R}_{\text{PVG}}$,$\overline{\mathcal{R}_{\text{PVG}}}$);

DEC_BOX p 1 ($\mathcal{R}_{\text{WTH}}$,$\overline{\mathcal{R}_{\text{WTH}}}$)]]

Theorem 5.12. *Verification of Capacity Outage 17.5 MW*

$$\vdash \texttt{COPT\_17\_5\_MW}\ \mathcal{R}_{\text{PVA}}\ \mathcal{R}_{\text{WTB}}\ \mathcal{R}_{\text{PVC}}\ \mathcal{R}_{\mathcal{WTD}}\ \mathcal{R}_{\text{PVE}}\ \mathcal{R}_{\text{WTF}}\ \mathcal{R}_{\text{PVG}}\ \mathcal{R}_{\text{WTH}}\ \texttt{p} = $$

$$\Big(\big(\mathrm{e}^{(-\lambda_{PV\_A1}t)} \times \mathrm{e}^{(-\lambda_{PV\_A2}t)} \times \mathrm{e}^{(-\lambda_{PV\_A3}t)} \times \mathrm{e}^{(-\lambda_{PV\_A4}t)} \times \mathrm{e}^{(-\lambda_{PV\_A5}t)}\big) \times$$

$$\big(\texttt{1 - } (1-\mathrm{e}^{(-\lambda_{WT\_B1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_B4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_C1}t)} \times \mathrm{e}^{(-\lambda_{PV\_C2}t)} \times \mathrm{e}^{(-\lambda_{PV\_C3}t)} \times \mathrm{e}^{(-\lambda_{PV\_C4}t)} \times \mathrm{e}^{(-\lambda_{PV\_C5}t)}\big) \times$$

$$\big(\texttt{1 - } (1-\mathrm{e}^{(-\lambda_{WT\_D1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_D4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_E1}t)} \times \mathrm{e}^{(-\lambda_{PV\_E2}t)} \times \mathrm{e}^{(-\lambda_{PV\_E3}t)} \times \mathrm{e}^{(-\lambda_{PV\_E4}t)} \times \mathrm{e}^{(-\lambda_{PV\_E5}t)}\big) \times$$

$$\big(\texttt{1 - } (1-\mathrm{e}^{(-\lambda_{WT\_F1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_F4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_G1}t)} \times \mathrm{e}^{(-\lambda_{PV\_G2}t)} \times \mathrm{e}^{(-\lambda_{PV\_G3}t)} \times \mathrm{e}^{(-\lambda_{PV\_G4}t)} \times \mathrm{e}^{(-\lambda_{PV\_G5}t)}\big) \times$$

$$\big((1-\mathrm{e}^{(-\lambda_{WT\_H1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H2}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_H3}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H5}t)})\big)\ \texttt{+}\ \ldots\ \texttt{+}\ \ldots\ \texttt{+}\ \ldots\big)\Big)$$

Definition 5.9. *Capacity Outage 35 MW*

$$\vdash \texttt{COPT\_35\_MW}\ \mathcal{R}_{\text{PVA}}\ \mathcal{R}_{\text{WTB}}\ \mathcal{R}_{\text{PVC}}\ \mathcal{R}_{\mathcal{WTD}}\ \mathcal{R}_{\text{PVE}}\ \mathcal{R}_{\text{WTF}}\ \mathcal{R}_{\text{PVG}}\ \mathcal{R}_{\text{WTH}}\ \texttt{p} = $$

$$\mathrm{Prob}_{X}^{CCD\lightning}\ \texttt{p}$$

$$\texttt{[[DEC\_BOX p 1 (}\mathcal{R}_{\text{PVA}}\texttt{,}\overline{\mathcal{R}_{\text{PVA}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\text{WTB}}\texttt{,}\overline{\mathcal{R}_{\text{WTB}}}\texttt{);}$$

$$\texttt{DEC\_BOX p 1 (}\mathcal{R}_{\text{PVC}}\texttt{,}\overline{\mathcal{R}_{\text{PVC}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\text{WTD}}\texttt{,}\overline{\mathcal{R}_{\text{WTD}}}\texttt{);}$$

$$\texttt{DEC\_BOX p 1 (}\mathcal{R}_{\text{PVE}}\texttt{,}\overline{\mathcal{R}_{\text{PVE}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\text{WTF}}\texttt{,}\overline{\mathcal{R}_{\text{WTF}}}\texttt{);}$$

$$\texttt{DEC\_BOX p 1 (}\mathcal{R}_{\text{PVG}}\texttt{,}\overline{\mathcal{R}_{\text{PVG}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\text{WTH}}\texttt{,}\overline{\mathcal{R}_{\text{WTH}}}\texttt{)];}$$

$$\vdots$$

$$\texttt{[DEC\_BOX p 0 (}\mathcal{R}_{\text{PVA}}\texttt{,}\overline{\mathcal{R}_{\text{PVA}}}\texttt{); DEC\_BOX p 0 (}\mathcal{R}_{\text{PVC}}\texttt{,}\overline{\mathcal{R}_{\text{PVC}}}\texttt{);}$$

$$\texttt{DEC\_BOX p 1 (}\mathcal{R}_{\text{PVE}}\texttt{,}\overline{\mathcal{R}_{\text{PVE}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\text{WTF}}\texttt{,}\overline{\mathcal{R}_{\text{WTF}}}\texttt{);}$$

$$\texttt{DEC\_BOX p 1 (}\mathcal{R}_{\text{PVG}}\texttt{,}\overline{\mathcal{R}_{\text{PVG}}}\texttt{); DEC\_BOX p 1 (}\mathcal{R}_{\text{WTH}}\texttt{,}\overline{\mathcal{R}_{\text{WTH}}}\texttt{)]]}$$

Theorem 5.13. *Verification of Capacity Outage 35 MW*

$$\vdash \texttt{COPT\_35\_MW}\ \mathcal{R}_{\text{PVA}}\ \mathcal{R}_{\text{WTB}}\ \mathcal{R}_{\text{PVC}}\ \mathcal{R}_{\mathcal{WTD}}\ \mathcal{R}_{\text{PVE}}\ \mathcal{R}_{\text{WTF}}\ \mathcal{R}_{\text{PVG}}\ \mathcal{R}_{\text{WTH}}\ \texttt{p =}$$

$$\Big(\big(\mathrm{e}^{(-\lambda_{PV\_A1}t)} \times \mathrm{e}^{(-\lambda_{PV\_A2}t)} \times \mathrm{e}^{(-\lambda_{PV\_A3}t)} \times \mathrm{e}^{(-\lambda_{PV\_A4}t)} \times \mathrm{e}^{(-\lambda_{PV\_A5}t)}\big) \times$$

$$\big(\texttt{1 - } (1-\mathrm{e}^{(-\lambda_{WT\_B1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_B4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_B5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_C1}t)} \times \mathrm{e}^{(-\lambda_{PV\_C2}t)} \times \mathrm{e}^{(-\lambda_{PV\_C3}t)} \times \mathrm{e}^{(-\lambda_{PV\_C4}t)} \times \mathrm{e}^{(-\lambda_{PV\_C5}t)}\big) \times$$

$$\big(\texttt{1 - } (1-\mathrm{e}^{(-\lambda_{WT\_D1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_D4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_D5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_E1}t)} \times \mathrm{e}^{(-\lambda_{PV\_E2}t)} \times \mathrm{e}^{(-\lambda_{PV\_E3}t)} \times \mathrm{e}^{(-\lambda_{PV\_E4}t)} \times \mathrm{e}^{(-\lambda_{PV\_E5}t)}\big) \times$$

$$\big((1-\mathrm{e}^{(-\lambda_{WT\_F1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_F4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_F5}t)})\big) \times$$

$$\big(\mathrm{e}^{(-\lambda_{PV\_G1}t)} \times \mathrm{e}^{(-\lambda_{PV\_G2}t)} \times \mathrm{e}^{(-\lambda_{PV\_G3}t)} \times \mathrm{e}^{(-\lambda_{PV\_G4}t)} \times \mathrm{e}^{(-\lambda_{PV\_G5}t)}\big) \times$$

$$\big((1-\mathrm{e}^{(-\lambda_{WT\_H1}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H2}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H3}t)}) \times$$

$$(1-\mathrm{e}^{(-\lambda_{WT\_H4}t)}) \times (1-\mathrm{e}^{(-\lambda_{WT\_H5}t)})\big)\ \texttt{+ ... + ... + ...}\ \big)\Big)$$

Similarly, we verified `COPT_0_MW`, `COPT_52_5_MW`, `COPT_70_MW` corresponding to the capacity outage probabilities 0 MW, 52.5 MW and 70 MW, of the smart power grid, respectively. Moreover, we can verify the energy indices ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR, for the interconnected MGs shown in Figure 5.6 using Definitions 4.15-4.24 (see Section 4.3.1). For example. we can verify the generated complex mathematical expression of energy index ASAI using Definition 4.18 as:

1. $\mathit{Prob}\ (\text{MG}_1\lightning) = \sum Pr_{\text{Paths}}(28-54, 55-81)$
2. $\mathit{Prob}\ (\text{MG}_2\lightning) = \sum Pr_{\text{Paths}}(10-27, 37-54, 64-81)$
3. $\mathit{Prob}\ (\text{MG}_3\lightning) = \sum Pr_{\text{Paths}}(4-9, 13-18, 22-27, \ldots, 67-72, 76-81)$
4. $\mathit{Prob}\,(\text{MG}_4\lightning) = \sum Pr_{\text{Paths}}(2,3,5,6,8,9,11,12,14,\ldots,71,72,74,75,77,78,80,81)$

Theorem 5.14. *Verification of of Smart Power Grid Energy Index ASAI*

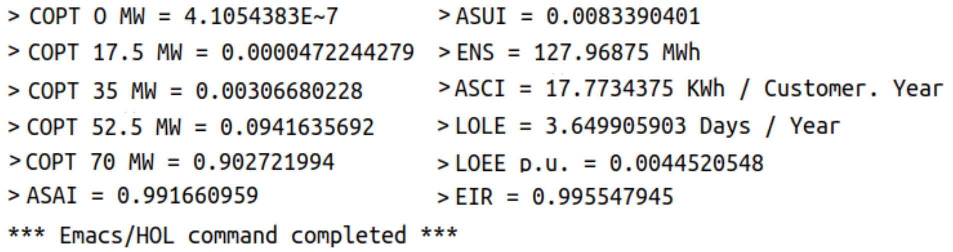
$$
\begin{aligned}
&\vdash \texttt{Smart\_Power\_Grid\_ASAI =} \\
&\Bigg[(\texttt{CN\_MG1 + CN\_MG2 + CN\_MG3 + CN\_MG4}) \times \texttt{8760 -} \\
&\Bigg(\Bigg(\Big(e^{(-\lambda_{PV\_A1}t)} \times e^{(-\lambda_{PV\_A2}t)} \times e^{(-\lambda_{PV\_A3}t)} \times e^{(-\lambda_{PV\_A4}t)} \times e^{(-\lambda_{PV\_A5}t)}\Big) \times \\
&\quad \Big((1-e^{(-\lambda_{WT\_B1}t)}) \times (1-e^{(-\lambda_{WT\_B2}t)}) \times (1-e^{(-\lambda_{WT\_B3}t)}) \times \\
&\quad\ \ (1-e^{(-\lambda_{WT\_B4}t)}) \times (1-e^{(-\lambda_{WT\_B5}t)})\Big) \times \\
&\quad \Big(e^{(-\lambda_{PV\_C1}t)} \times e^{(-\lambda_{PV\_C2}t)} \times e^{(-\lambda_{PV\_C3}t)} \times e^{(-\lambda_{PV\_C4}t)} \times e^{(-\lambda_{PV\_C5}t)}\Big) \times \\
&\quad \Big(\texttt{1 -} (1-e^{(-\lambda_{WT\_D1}t)}) \times (1-e^{(-\lambda_{WT\_D2}t)}) \times (1-e^{(-\lambda_{WT\_D3}t)}) \times \\
&\qquad\quad (1-e^{(-\lambda_{WT\_D4}t)}) \times (1-e^{(-\lambda_{WT\_D5}t)})\Big) \times \ldots \times \\
&\quad \Big(\texttt{1 -} (1-e^{(-\lambda_{WT\_F1}t)}) \times (1-e^{(-\lambda_{WT\_F2}t)}) \times (1-e^{(-\lambda_{WT\_F3}t)}) \times \\
&\qquad\quad (1-e^{(-\lambda_{WT\_F4}t)}) \times (1-e^{(-\lambda_{WT\_F5}t)})\Big) \times \\
&\quad \Big(e^{(-\lambda_{PV\_G1}t)} \times e^{(-\lambda_{PV\_G2}t)} \times e^{(-\lambda_{PV\_G3}t)} \times e^{(-\lambda_{PV\_G4}t)} \times e^{(-\lambda_{PV\_G5}t)}\Big) \times \\
&\quad \Big(\texttt{1 -} (1-e^{(-\lambda_{WT\_H1}t)}) \times (1-e^{(-\lambda_{WT\_H2}t)}) \times (1-e^{(-\lambda_{WT\_H3}t)}) \times \\
&\qquad\quad (1-e^{(-\lambda_{WT\_H4}t)}) \times (1-e^{(-\lambda_{WT\_H5}t)})\Big) \texttt{ + } \ldots\Bigg) \times \texttt{MTTR\_MG1} \times \texttt{CN\_MG1 +} \\
&\quad \ldots \texttt{ + } \ldots \texttt{ + } \ldots \texttt{ + } \ldots \texttt{ +} \\
&\quad \Bigg(\Big(e^{(-\lambda_{PV\_A1}t)} \times e^{(-\lambda_{PV\_A2}t)} \times e^{(-\lambda_{PV\_A3}t)} \times e^{(-\lambda_{PV\_A4}t)} \times e^{(-\lambda_{PV\_A5}t)}\Big) \times \ldots \times \\
&\quad \Big(e^{(-\lambda_{PV\_C1}t)} \times e^{(-\lambda_{PV\_C2}t)} \times e^{(-\lambda_{PV\_C3}t)} \times e^{(-\lambda_{PV\_C4}t)} \times e^{(-\lambda_{PV\_C5}t)}\Big) \times \\
&\quad \Big(\texttt{1 -} (1-e^{(-\lambda_{WT\_D1}t)}) \times (1-e^{(-\lambda_{WT\_D2}t)}) \times (1-e^{(-\lambda_{WT\_D3}t)}) \times \\
&\qquad\quad (1-e^{(-\lambda_{WT\_D4}t)}) \times (1-e^{(-\lambda_{WT\_D5}t)})\Big) \times \ldots \times \\
&\quad \Big(\texttt{1 -} (1-e^{(-\lambda_{WT\_F1}t)}) \times (1-e^{(-\lambda_{WT\_F2}t)}) \times (1-e^{(-\lambda_{WT\_F3}t)}) \times \\
&\qquad\quad (1-e^{(-\lambda_{WT\_F4}t)}) \times (1-e^{(-\lambda_{WT\_F5}t)})\Big) \times \\
&\quad \Big(e^{(-\lambda_{PV\_G1}t)} \times e^{(-\lambda_{PV\_G2}t)} \times e^{(-\lambda_{PV\_G3}t)} \times e^{(-\lambda_{PV\_G4}t)} \times e^{(-\lambda_{PV\_G5}t)}\Big) \times \\
&\quad \Big((1-e^{(-\lambda_{WT\_H1}t)}) \times (1-e^{(-\lambda_{WT\_H2}t)}) \times (1-e^{(-\lambda_{WT\_H3}t)}) \times \\
&\quad\ \ (1-e^{(-\lambda_{WT\_H4}t)}) \times (1-e^{(-\lambda_{WT\_H5}t)})\Big) \texttt{ + } \ldots\Big) \times \texttt{MTTR\_MG4} \times \texttt{CN\_MG4}\Bigg)\Bigg] \\
&\quad \texttt{/ (CN\_MG1 + CN\_MG2 + CN\_MG3 + CN\_MG4)} \times \texttt{8760}
\end{aligned}
$$

The proof of the above-verified energy expressions at the subsystem level was conducted using HOL4 tactics like `match_mp_tac`, `q.exists_tac` and `irule` [68].

5.4.3 Numerical Results

Considering the failure rate of the solar PV generation units, i.e., λ_{PV_A1}-λ_{PV_A5}, λ_{PV_C1}-λ_{PV_C5}, λ_{PV_E1}-λ_{PV_E5} and λ_{PV_G1}-λ_{PV_G5}, are 0.73 per year with MTTR of 40 hours [103]. Similarly, the failure rates of the WT generation units, i.e., λ_{WT_B1}-λ_{WT_B5}, λ_{WT_D1}-λ_{WT_D5}, λ_{WT_F1}-λ_{WT_F5} and λ_{WT_H1}-λ_{WT_H5}, are 0.66 per year with MTTR of 55 hours [104]. Also, assuming the numbers of customers served CN_{MG1}, CN_{MG2}, CN_{MG3}, CN_{MG4} at $Micro\ Grid_1$, $Micro\ Grid_2$, $Micro\ Grid_3$, $Micro\ Grid_4$ are 1600, 2000, 1700 and 1900 customers, respectively. The reliability study for the interconnected MGs is undertaken for 1 year (365 days), i.e., $t = 8760$ hours. Based on the given data, we now evaluate the capacity outage probability table COPT as well as the reliability and energy indices ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR for the SG power system shown in Figure 5.6 using: (1) our HOL4 analysis; (2) Paper-and-pencil analysis; and (3) MATLAB Monte-Carlo Simulation (MCS).

1. ***HOL4 Analysis:*** we define SML functions [93] to numerically evaluate the verified HOL4 reliability and energy expressions as shown in Figure 5.8.



```
> COPT O MW = 4.1054383E~7         > ASUI = 0.0083390401
> COPT 17.5 MW = 0.0000472244279  > ENS = 127.96875 MWh
> COPT 35 MW = 0.00306680228      > ASCI = 17.7734375 KWh / Customer. Year
> COPT 52.5 MW = 0.0941635692     > LOLE = 3.649905903 Days / Year
> COPT 70 MW = 0.902721994        > LOEE p.u. = 0.0044520548
> ASAI = 0.991660959              > EIR = 0.995547945
*** Emacs/HOL command completed ***
```

Figure 5.8: HOL4 Analysis: Micro-Grids Reliability/Energy Indices Results

2. *Manual Analysis:* we manually develop the CCD model at the subsystem level on a paper and calculate the COPT as well as the energy indices by determining the probabilities of the corresponding consequence paths.

3. *MATLAB Monte-Carlo Simulation:* we use the cause consequence analysis at the subsystem level of interconnected MGs and the exponential distribution for all generating PV/WT units, then we obtain a variation in the obtained results for energy indices with a tolerance error between 5-10%.

A comparison between the results of the COPT and the reliability indices ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR for the interconnected MGs power system is summarized in Tables 5.2 and 5.3, respectively. It can be noticed that the energy indices of the interconnected MGs power system obtained from our formal analysis are equivalent to the corresponding ones calculated using the manual paper-and-pencil cause consequence analysis. Note that during the mathematical analysis and due to the large-size of the application, some errors that we inadvertently made were caught through one-to-one comparison with the HOL4 verified analysis results. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results of ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR at every generation of

Table 5.2: Capacity Outage Probability Table (COPT)

Smart Power Grid Capacity		Probability Evaluation		
Out	In	Manual	MATLAB	HOL4
0 MW	70 MW	41.02e-8	60.15e-6	41.0154383e-8
17.5 MW	52.5 MW	47.22e-6	20.64e-5	47.2244279e-6
35 MW	35 MW	30.67e-4	60.41e-3	30.6680228e-4
52.5 MW	17.5 MW	94.16e-3	68.62e-3	94.1635692e-3
70 MW	0 MW	90.27e-2	87.07e-2	90.2721994e-2
CPU Time (Seconds)		–	76.582	6.349

Table 5.3: Reliability Indices for the Micro-Grids

Reliability and Energy Indices	Manual	MATLAB	HOL4
ASAI	0.992	0.97	0.991660959
ASUI	0.008	0.03	0.008339041
ENS (MWh)	127.97	130.28	127.9687500
ASCI (KWh/Customer.yr)	17.77	18.09	17.77343750
LOLE (days/year)	3.65	4.02	3.649905903
LOEE p.u.	0.0045	0.0086	0.004520548
EIR	0.9955	0.914	0.995547945
CPU Time (Seconds)	–	123.916	9.477

a random number U with errors between 5-10 %. Tables 5.2 and 5.3 show the best-obtained results of ASAI, ASUI, ENS, ASCI, LOLE, LOEE and EIR using MCS with the least errors after multiple runs of the algorithm. This above comparison validates our analysis results as well as the computation of all COPT and energy indices with a much faster CPU time with respect to MATLAB (13X), as shown in Tables 5.2 and 5.3. Also, the modeling time of the smart power grid using MATLAB was greater than the time needed for HOL4, but both consumed much less time (a matter of hours) than the manual analysis that needed a few days to construct the model.

5.5 Summary

In this chapter, we described the formalization of the RBD/ET-based cause consequence analysis. We provided reasoning support for formal probabilistic analysis of *multi-level* CCD paths with new proposed mathematical formulations and also their formalization in HOL4. The HOL4 proofs were conducted based on multiple levels of induction on lists and our developed theories for ET and FT-CCD as well as the existing RBD theory in HOL4. The proof-script of the formalization work presented in this section amounts to about 5,500 lines of HOL4 code [93]. We conducted the RBD/ET-based cause consequence analysis of a realistic smart power grid consisting of four interconnected Micro-Grids incorporating 100% carbon-neutral power generation and validate our formal reliability and energy indices results with the corresponding ones obtained through MATLAB MCS and manual analysis.

A limitation of Cause consequence analysis is that we can only assign two states to each subsystem, i.e., `YES` (success) and `NO` (failure). If planners/designers need to assign *multi-state* of complete/partial failure and reliability to each subsystem during the reliability analysis of realistic systems, then we need a hierarchical graph structure based on ETs, such as Functional Block Diagrams (FBD) for the probabilistic risk assessment. In the next chapter, we present the formalization of FBDs in HOL4.

Chapter 6

Formal Functional Block Diagram Reliability Analysis

In this chapter, we describe the formalization of Functional Block Diagrams (FBD) in HOL4. We formalize the FBD basic modeling functions and verify the related FBD probabilistic theorems. We provide reasoning support for formal probabilistic risk assessment of multi-levels FBDs, which can mathematically analyze complex hierarchical ET structures at subsystems component level that are composed of multi-states of failure and reliability. Lastly, we conduct the formal FBD reliability analysis of a nuclear power plant with multiple-levels decomposition of the boiling water reactor.

6.1 FBD Formalization

We start the formalization of FBDs by defining a modeling function for its basic element FB, using Definition 3.4, as shown in Figure 6.1, in HOL4 as follows:

Definition 6.1. *Functional Block*

$\vdash \mathcal{FB}\ (\mathcal{S}::\mathcal{I}_{\mathcal{N}}) = \mathcal{I}_{\mathcal{N}} \bigotimes_{\mathrm{L}}^{\mathcal{N}} \mathcal{S}$

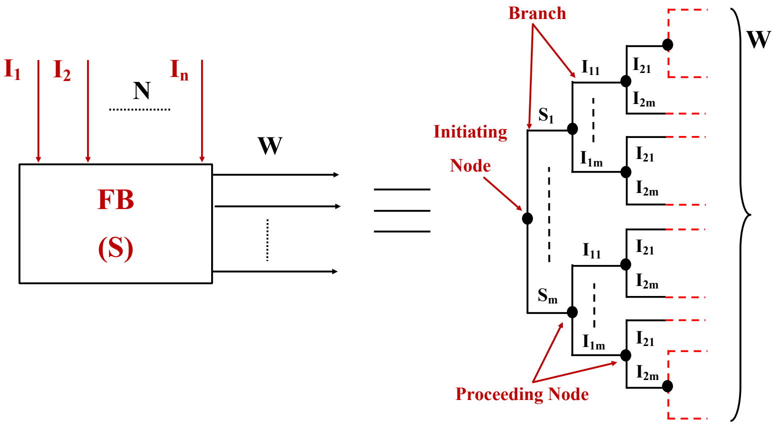


Figure 6.1: An FB Equal to a Complete ET model

where $\mathcal{S}$ is a list of all subsystem internal components failure and success states and $\mathcal{I}_{\mathcal{N}}$ is a *two-dimensional* list of all inputs states that affect the subsystem FB, i.e., $\mathcal{I}_{\mathcal{N}} = [[\mathcal{I}_1]; [\mathcal{I}_2]; [\mathcal{I}_3];\ldots; [\mathcal{I}_n]]$. The function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ takes the input lists $\mathcal{I}_{\mathcal{N}}$ and internal state list $\mathcal{S}$ and returns an output list $\mathcal{W}$ containing all possible joint events ω_{jk} for the occurrence of $\mathcal{I}_{\mathcal{N}}$ and $\mathcal{S}$ together. Remark that the above definition provides the modeling of FBs associated with *multi-state* subsystem components and is based on any given probabilistic distribution. Definition 6.1 can now be used to construct an FBD model, i.e. the first step of the FBD analysis described in Section 2.2. Also, we define a *generic three-dimensional* function $\mathcal{FB}_{\mathcal{N}}$ that takes multi-level FBs, where each FB takes an arbitrary two-dimensional list of n inputs and then generates the corresponding complete FBD model to obtain all possible risk consequences of failure and reliability, as shown in Figure 6.2, in HOL4 as:

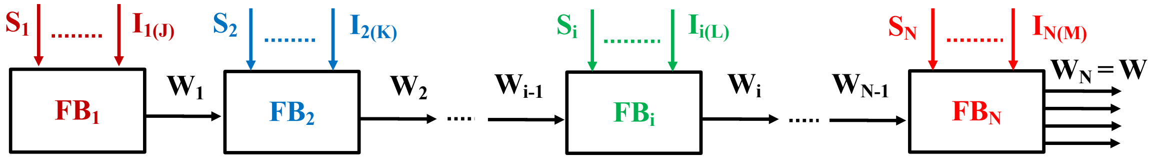


Figure 6.2: Complete FBD Model of Multi-Level FBs Connected Together

Definition 6.2. *Three Dimensional Multi-Level Functional Block Modeling*

$\vdash \mathcal{FB}_{\mathcal{N}}\ \left(\mathcal{SI}_1\texttt{::}\mathcal{SI}_2\texttt{::}\mathcal{SI}_{\mathcal{N}}\right)\ \texttt{=}\ \mathcal{FB}\ \left(\texttt{MAP}\ (\lambda\texttt{a}.\ \ \mathcal{FB}\ \texttt{a})\ (\mathcal{SI}_1\texttt{::}\mathcal{SI}_2\texttt{::}\mathcal{SI}_{\mathcal{N}})\right)$

The second step of the FBD analysis is the model ET diagrams for all FBs. Therefore, we define a function $\mathcal{FB}_{ET}$ to obtain an ET model of a specific functional block $\mathcal{FB}_j$ and a recursive function $\mathcal{FB}_{ET}^{\mathcal{N}}$ to construct multiple ET models for consecutive *multi-level* FBs, respectively, in HOL4 as follows:

Definition 6.3. *Functional Block ET*

$\vdash \mathcal{FB}_{ET}\ \mathcal{FB}_j\ \texttt{=}\ \texttt{ETREE}\ (\texttt{NODE}\ \mathcal{FB}_j)$

Definition 6.4. *Multiple Functional Block ET*

$\vdash \mathcal{FB}_{ET}^{\mathcal{N}}\ (\mathcal{FB}_1\texttt{::}\mathcal{FB}_{\mathcal{N}})\ \texttt{=}\ \mathcal{FB}_{ET}\ \mathcal{FB}_1\texttt{::}\mathcal{FB}_{ET}^{\mathcal{N}}\ \mathcal{FB}_{\mathcal{N}}$

In order to verify the correctness of the above-mentioned functions, we formalize the following FBD modeling properties [8], in HOL4 as follows:

Property 1: An ET diagram of an FB model having $\mathcal{N}$ input lists $\mathcal{I}_{\mathcal{N}}$ and an internal state list $\mathcal{S}$ can be *split* as connected individual FBs for all lists associated with the FB model, as shown in Figure 6.3, in HOL4 as:

Theorem 6.1. *Splitting Single Functional Block*

$\vdash \mathcal{FB}_{ET}\ \left(\mathcal{FB}\ (\mathcal{S}\texttt{::}\mathcal{I}_{\mathcal{N}})\right)\ \texttt{=}\ \mathrm{ET}_{PATH}\ \texttt{p}\ \left(\mathcal{FB}_{ET}^{\mathcal{N}}\ (\mathcal{S}\texttt{::}\mathcal{I}_{\mathcal{N}})\right)$

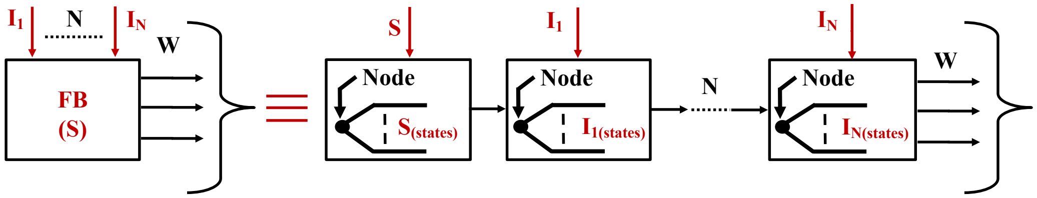


Figure 6.3: An FB of $\mathcal{N}$ Inputs Split into Connected Individual FBs

Property 2: The *commutativity* and *associativity* properties of two consecutive FBs consisting of $\mathcal{N}$ input lists $\mathcal{I}_{\mathcal{N}}$, as shown in Figure 6.4, in HOL4 as:

Theorem 6.2. *Commutativity and Associativity of Two Consecutive FBs*

$\vdash$ $\mathcal{FB}_{ET}$ $\big(\mathcal{FB}$ $(\mathcal{I}_1::\mathcal{I}_{\mathcal{N}})$ $\bigotimes_{\text{L}}$ $\mathcal{I}_2\big)$ = $\mathcal{FB}_{ET}$ $\big(\mathcal{I}_1$ $\bigotimes_{\text{L}}$ $(\mathcal{FB}$ $(\mathcal{I}_2::\mathcal{I}_{\mathcal{N}}))\big)$

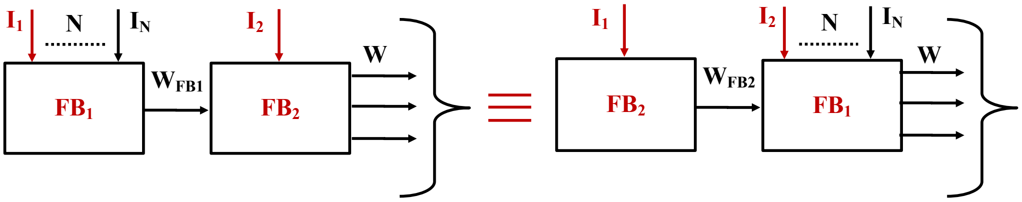


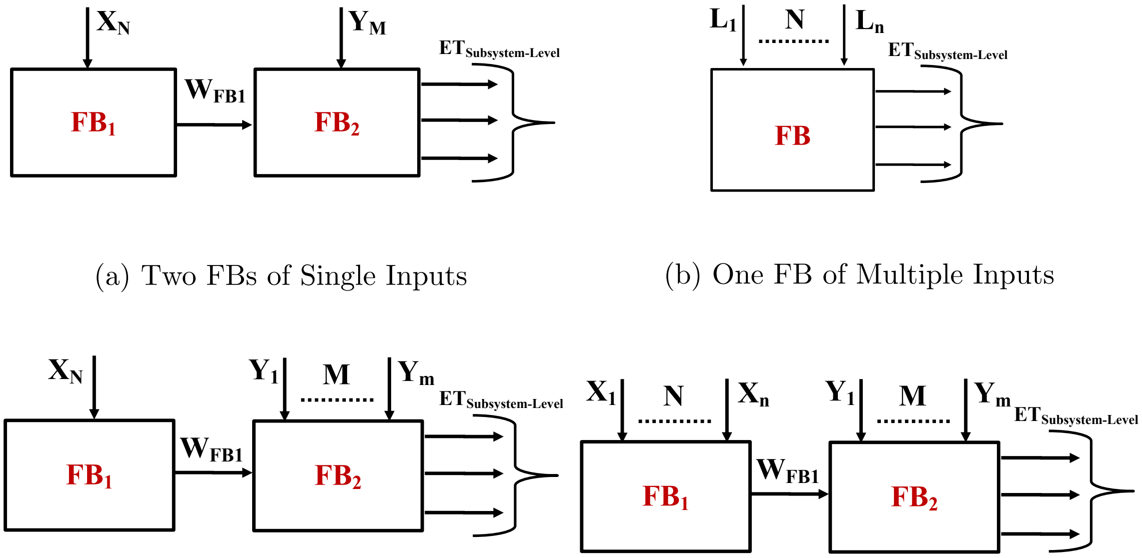
Figure 6.4: Commutativity and Associativity of Two Consecutive FBs

The next step of the FBD analysis is to reduce and partition the ET model for each FB model (see Section 2.2). Since the outcome of $\mathcal{FB}$ is a list of all risk events ω_{jk} scenarios, we can use the same reduction function $\boxtimes^{\mathcal{N}}$ and partitioning function $\boxplus$ for ET analysis (i.e., Definitions 3.8 and 3.9, respectively) to reduce the ET model and partition a collection of consequence events that end with the same risk events.

6.2 Formal FBD Probabilistic Analysis

The last step of FBD reliability analysis is to determine the probability of each ET consequence risk scenario at the subsystem-level that could occur in a complex system. Based on the ET probabilistic theorems in Section 3.1.3 and the formal FBD modeling theorems (Theorems 6.1-6.2), we have verified the FBD probabilistic properties for different configurations of FB connections [8], in HOL4 as follows:

Property 3: Two consecutive FBs corresponding to two subsystems of single input lists $\text{X}_{\mathcal{N}}$ and $\text{Y}_{\mathcal{M}}$, where each list consists of multi-states of complete/partial failure and reliability, as shown in Figure 6.5(a). Then, the probability of the Cartesian product function $\bigotimes_{\text{L}}$ for two $\mathcal{FB}$ lists is verified as the multiplication of the sum of the individual probabilities of all the events associated with each list, in HOL4 as:



(a) Two FBs of Single Inputs

(b) One FB of Multiple Inputs

(c) FB of Single Input with FB of Multiple Inputs

(d) Two FBs of Two Multiple Inputs

Figure 6.5: Different Configurations of Connected FBs

Theorem 6.3. *Two FBs of Single Inputs*

$\vdash \texttt{prob p} \left(\mathcal{FB}_{ET}\ (\mathrm{X}_{\mathcal{N}} \bigotimes_{\mathrm{L}} \mathrm{Y}_{\mathcal{M}})\right) = \sum\ (\mathrm{Pr}_{\mathrm{L}}\ \texttt{p}\ \mathrm{X}_{\mathcal{N}}) \times \sum\ (\mathrm{Pr}_{\mathrm{L}}\ \texttt{p}\ \mathrm{Y}_{\mathcal{M}})$

where the function $\sum$ takes a list Y_M and returns the sum of the elements of a list, i.e., $Y_1 + Y_2 + Y_3 + Y_4 + \cdots + Y_{n-1} + Y_n$ while the function Pr_{L} returns the probabilities of the elements of a list, i.e., $[Pr(Z_1), Pr(Z_2), , \ \ldots, Pr(Z_{n-1}), Pr(Z_n)]$.

Property 4: Single FB of multiple input lists $\mathrm{L}_{\mathcal{N}}$, i.e., [[L_1]; [L_2]; [L_3];...; [L_n]], where each list consists of multi-states of complete/partial failure and reliability, as shown in Figure 6.5(b). A generic probabilistic formulation is verified as the product of the sum of each component list probabilities, in HOL4 as:

Theorem 6.4. *One FB of Multiple Inputs*

$\vdash \texttt{prob p} \left(\mathcal{FB}_{ET}\ (\mathcal{FB}\ (\mathrm{L}_1\texttt{::}\mathrm{L}_{\mathcal{N}}))\right) = \prod\ (\sum_{\mathrm{prob}}\ \texttt{p}\ (\mathrm{L}_1\texttt{::}\mathrm{L}_{\mathcal{N}}))$

where the function $\sum_{\mathrm{prob}}$ is used to recursively apply the functions Pr_{L} and $\sum$ on a given two-dimensional list $\mathrm{L}_{\mathcal{N}}$.

Property 5: A probabilistic formulation for one FB of one list and another with multiple lists, as shown in Figure 6.5(c), is verified as the multiplication of their probabilities, in HOL4 as:

Theorem 6.5. *FB of Single Input with FB of Multiple Inputs*

$\vdash \texttt{prob p} \left(\mathcal{FB}_{ET}\ \texttt{(}\mathrm{X}_{\mathcal{N}}\ \bigotimes_{\mathrm{L}}\ \texttt{(}\mathcal{FB}\ \texttt{(}\mathrm{Y}_1\texttt{::}\mathrm{Y}_m\texttt{)))}\right)\ \texttt{=}$

$\quad \sum\ \texttt{(}\mathrm{Pr}_{\mathrm{L}}\ \texttt{p}\ \mathrm{X}_{\mathcal{N}}\texttt{)}\ \times\ \prod\ \texttt{(}\sum_{\mathrm{prob}}\ \texttt{p}\ \texttt{(}\mathrm{Y}_1\texttt{::}\mathrm{Y}_m\texttt{))}$

Property 6: A probabilistic formulation for two FBs of multiple input lists (Figure 6.5(d)) is verified as the multiplication of both probabilities, in HOL4 as:

Theorem 6.6. *Two FBs of Multiple Inputs*

$\vdash \texttt{prob p} \left(\mathcal{FB}_{ET}\ \left(\mathcal{FB}\ \texttt{(}\mathrm{X}_1\texttt{::}\mathrm{X}_m\texttt{)}\ \bigotimes_{\mathrm{L}}\ \mathcal{FB}\ \texttt{(}\mathrm{Y}_1\texttt{::}\mathrm{Y}_m\texttt{)}\right)\right)\ \texttt{=}$

$\quad \prod\ \texttt{(}\sum_{\mathrm{prob}}\ \texttt{p}\ \texttt{(}\mathrm{X}_1\texttt{::}\mathrm{X}_n\texttt{))}\ \times\ \prod\ \texttt{(}\sum_{\mathrm{prob}}\ \texttt{p}\ \texttt{(}\mathrm{Y}_1\texttt{::}\mathrm{Y}_m\texttt{))}$

The prime purpose of the above-mentioned formalization of FBDs is to build a reasoning support for the subsystem-level formal safety analysis of realistic complex systems within the sound environment of HOL4. In the next section, we present the formal FBD-based safety analysis of a nuclear power plant generation system to illustrate the applicability of our proposed formal approach.

6.3 Application: Nuclear Power Plant

A Nuclear Power Plant, as shown in Figure 6.6 [15], is composed of a boiling water reactor (BWR), control rods, a steam generator, a steam line, a turbine generator, a switchyard, cooling towers, a condenser and pumps [15]. The nuclear reactor heats the reactor coolant, which is water to pass through a steam generator and produces a steam flow in the steam line. The pressurized steam flow then goes to a

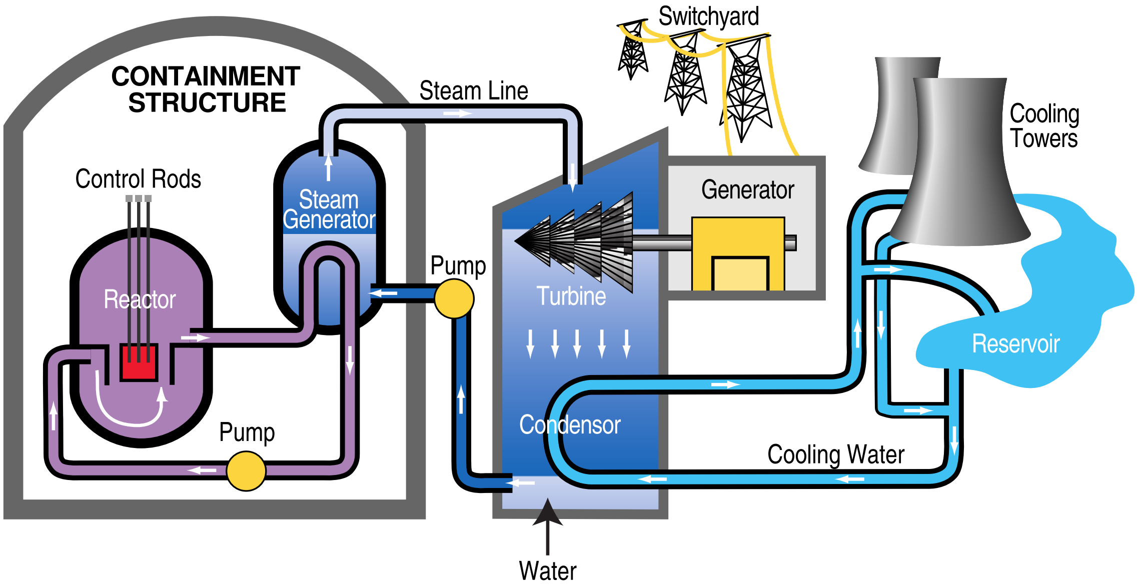
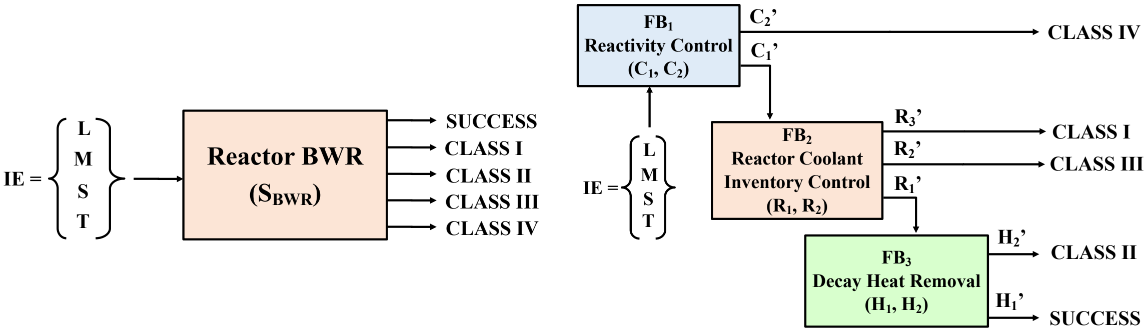


Figure 6.6: Nuclear Power Plant Structure

steam turbine, which starts to produce power and the remaining vapor is condensed through a condenser. The condenser is used to exchange heat through a secondary side, for instance, a river or a cooling tower. The condensed water is again pumped back to the steam generator and the cycle repeats. In the sequel, we use our formal FBD reliability analysis to determine the probabilities of all possible classes of accident events that can occur in the nuclear reactor.

6.3.1 Formal FBD Model

Figure 6.7(a) [105] depicts the system-level FBD of a Boiling Water Reactor (BWR) that can have one of the following sudden accident Initial Events (IE): (a) L: Large loss of coolant accident; (b) M: Medium loss of coolant accident; and (c) S: Small loss of coolant accident; and (d) T: Transient accident. Based on these IEs, there are four



(a) System-Level FBD of BWR (b) First-Level FBD of BWR

Figure 6.7: FBD of Nuclear Power Plant System

classes of accidents that can occur, as shown in Figure 6.7(a): (1) *CLASS I*: Containment intact when the nuclear reactor core melts at low pressure; (2) *CLASS II*: Containment failing when the nuclear reactor core melts; (3) *CLASS III*: Containment intact when the nuclear reactor core melts at high internal pressure; and (4) *CLASS IV*: Containment failing prior to the nuclear reactor core melting due to severe overpressure. The characteristic of each class is based on the melting time of the reactor's core, i.e., before or after the containment, as well as the pressure status when the containment fails. All these parameters affect the extent of the consequences of the radioactivity released in the surrounding environment. The system-level FBD analysis for the safety of the BWR system can be formally modeled, in HOL4 as:

Definition 6.5. *System Level FBD Model of Boiling Water Reactor*

$\vdash$ `System_Level_FBD_BWR` $[[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]]$

$[\mathrm{P}_{\mathrm{SUCCESS}};\mathrm{P}_{\mathrm{CLASS\_I}};\mathrm{P}_{\mathrm{CLASS\_II}};\mathrm{P}_{\mathrm{CLASS\_III}};\mathrm{P}_{\mathrm{CLASS\_IV}}]$ =

$\mathcal{FB}_{ET}$ $[\boxplus\ \mathrm{P}_{\mathrm{SUCCESS}}\ (\mathcal{FB}\ [[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]]);$

$\boxplus\ \mathrm{P}_{\mathrm{CLASS\_I}}\ (\mathcal{FB}\ [[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]]);$

$\boxplus\ \mathrm{P}_{\mathrm{CLASS\_II}}\ (\mathcal{FB}\ [[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]]);$

$\boxplus\ \mathrm{P}_{\mathrm{CLASS\_III}}\ (\mathcal{FB}\ [[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]]);$

$\boxplus\ \mathrm{P}_{\mathrm{CLASS\_IV}}\ (\mathcal{FB}\ [[\mathrm{L};\mathrm{M};\mathrm{S};\mathrm{T}];[\mathrm{S}_{\mathrm{BWR}}]])]$

To study the internal states of the reactor S_{BWR} hierarchically, the system-level FBD is decomposed into 3 major *first-level* FBs (Figure 6.7(b) [8]) as follows:

1. *Reactivity Control* (FB_1): It stops the chain reaction of the nuclear reactor. It is mainly controlled by the insertion of control rods, as shown in Figure 6.7(a). It has two internal states: (a) C_1 represents that the reactivity is successfully controlled; and (b) C_2 represents that the reactivity cannot be controlled.
2. *Reactor Coolant Inventory Control* (FB_2): It provides the reactor core with an adequate amount of coolant to maintain its necessary inventory. Two internal states are considered: (a) R_1 represents the successful functioning of the reactor coolant inventory control; and (b) R_2 the failure of the reactor coolant control.
3. *Decay Heat Removal* (FB_3): It removes the decay and the stored heat from the reactor core to the environment. It considers two internal states: (a) H_1 represents that the function of decay heat removal can be done successfully; and (b) H_2 represents the failure of decay heat removal.

We can formally define the decomposed *first-level* FBD model of the BWR system, as shown in Figure 6.7(b), in HOL4 as:

Definition 6.6. *First Level FBD Model of Boiling Water Reactor*

$\vdash$ $\texttt{Let}\ \mathcal{W}_{C'_1}\ \texttt{=}\ \boxplus\ P_{C'_1}\ \texttt{(}\mathcal{FB}\ \texttt{[[}L\texttt{;}M\texttt{;}S\texttt{;}T\texttt{];[}C_1\texttt{;}C_2\texttt{]])}$

$\quad\texttt{in FIRST\_LEVEL\_FBD\_BWR [[}L\texttt{;}M\texttt{;}S\texttt{;}T\texttt{];[}C_1\texttt{;}C_2\texttt{];[}R_1\texttt{;}R_2\texttt{];[}H_1\texttt{;}H_2\texttt{]]}$

$\qquad\qquad\qquad\texttt{[}P_{C'_1}\texttt{;}P_{C'_2}\texttt{;}P_{R'_1}\texttt{;}P_{R'_2}\texttt{;}P_{R'_3}\texttt{;}P_{H'_1}\texttt{;}P_{H'_2}\texttt{] =}$

$\quad\mathcal{FB}_{ET}\ \texttt{[}\boxplus\ P_{C'_2}\ \texttt{(}\mathcal{FB}\ \texttt{[[}L\texttt{;}M\texttt{;}S\texttt{;}T\texttt{];[}C_1\texttt{;}C_2\texttt{]]);}$

$\qquad\quad\boxplus\ P_{R'_2}\ \texttt{(}\mathcal{FB}\ \texttt{[}\mathcal{W}_{C'_1}\texttt{;[}R_1\texttt{;}R_2\texttt{]]);}$

$\qquad\quad\boxplus\ P_{R'_3}\ \texttt{(}\mathcal{FB}\ \texttt{[}\mathcal{W}_{C'_1}\texttt{;[}R_1\texttt{;}R_2\texttt{]]);}$

$\qquad\quad\boxplus\ P_{H'_2}\ \texttt{(}\mathcal{FB}\ \texttt{[}\boxplus\ P_{R'_1}\ \texttt{(}\mathcal{FB}\ \texttt{[}\mathcal{W}_{C'_1}\texttt{;[}R_1\texttt{;}R_2\texttt{]]);[}H_1\texttt{;}H_2\texttt{]]);}$

$\qquad\quad\boxplus\ P_{H'_1}\ \texttt{(}\mathcal{FB}\ \texttt{[}\boxplus\ P_{R'_1}\ \texttt{(}\mathcal{FB}\ \texttt{[}\mathcal{W}_{C'_1}\texttt{;[}R_1\texttt{;}R_2\texttt{]]);[}H_1\texttt{;}H_2\texttt{]])]}$

Now, we can decompose the *first-level* FBD of BWR to *multiple-levels* describing the details of BWR safety functions, as shown in Figure 6.8 [8] to obtain a complete 6,144 possible test cases ($4 \times 2 \times 3 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$). The decomposed FBD is constructed based on the nuclear power engineering knowledge to describe the system behavior, which can be summarized as follows [8]:

1. The process to control the reactor coolant inventory of BWR can be performed either at high or low pressure. The first priority is to conduct the control process at high pressure (FB_{21}), but if high pressure is not available, then the process should be performed at low pressure (FB_{23}) through a depressurization of the reactor coolant circuit (FB_{22}), as shown in Figure 6.8.
2. The integrity of the high-pressure reactor coolant inventory (FB_{21}) can be preserved through using either a feed-water Power Conversion System (PCS) (FB_{212}) or High Pressure Core Injection (HPCI) and Reactor Core Isolation Cooling (RCIC) (FB_{213}). This is done after the water relief operation (FB_{211}), which opens the safety valves enough for relieving the pressure from the circuit. The failure to relieve the pressure will lead to an undesirable break.
3. The low pressure reactor coolant inventory control (FB_{23}) is decomposed into three safety functions: (a) Low Pressure Coolant Injection (FB_{231}); (b) Emergency Coolant Injection (FB_{232}); and (c) Coolant Recirculation (FB_{233}).
4. Finally, the decay heat (FB_3) is removed from the reactor core using: (a) Direct Power Conversion (DPC) (FB_{31}); and (b) Residual Heat Removal (RHR) (FB_{32}), which transfer the decay heat to a heat-sink in the power station.

Each FB of the BWR can be assigned with a multi-state model for safety analysis (see Figure 3.1). We assume that each FB has two possible safety states only (correct functioning $\mathcal{X}_1$ and failure operation $\mathcal{X}_2$). Since the pressure relief process (FB_{211}) is a

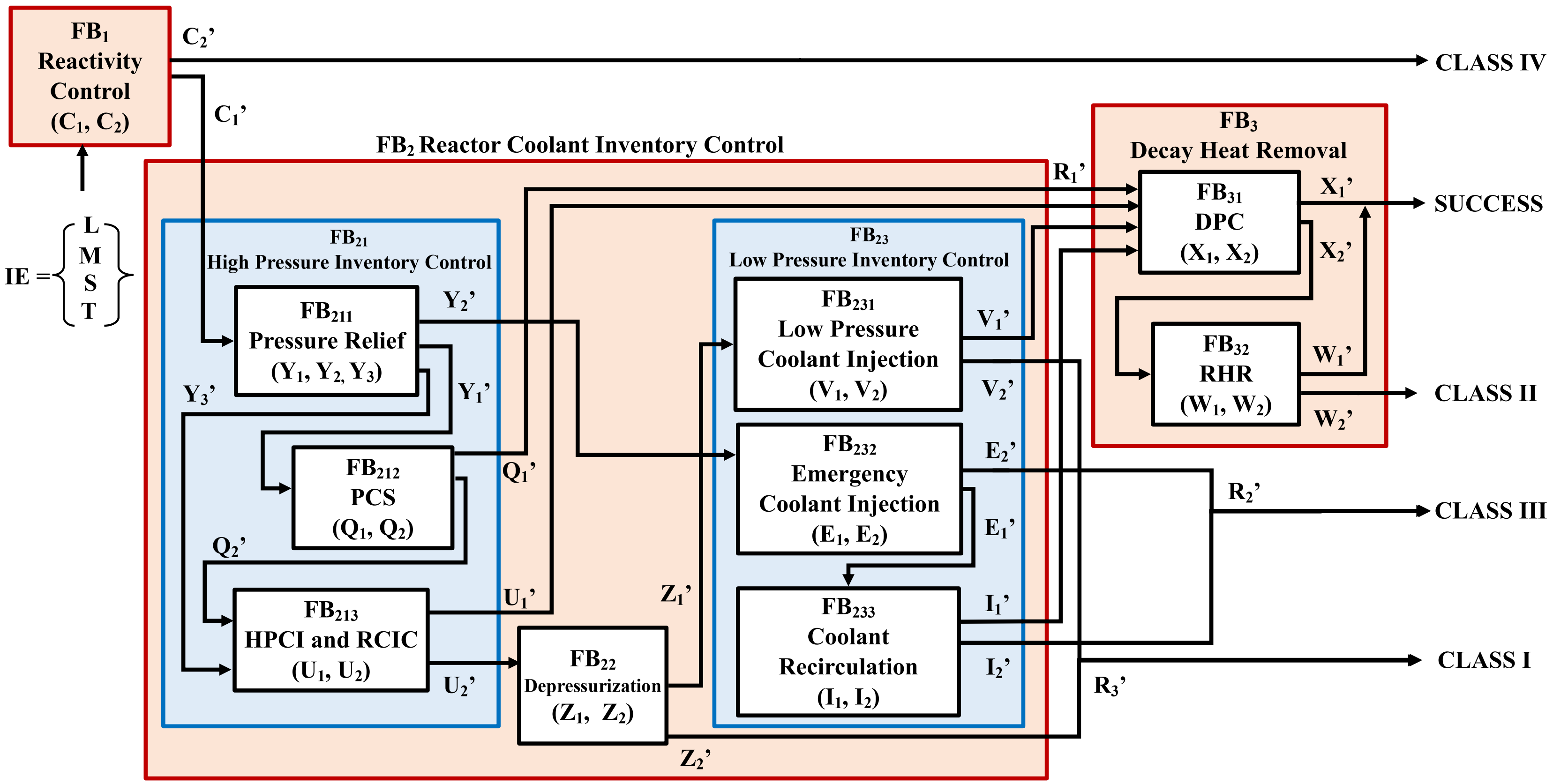


Figure 6.8: Multiple-Levels FBD of Boiling Water Reactor for Nuclear Power Plant

very critical process, it is represented by 3-state model (see Figure 3.1): (a) Y_1: Safety valve works correctly for pressure relief (opens and then recloses); (b) Y_2: Safety valve fails to open; and (c) Y_3: Safety valve works partly properly (opens but fails to recloses), as shown in Figure 6.8. Based on the above detailed description of the decomposed *multiple-levels* FBD of the nuclear power plant, we can formally describe its graphical FBD (Figure 6.8) associated with all the safety classes, in HOL4 as:

Definition 6.7. *Multiple-Levels FBD Model of Boiling Water Reactor*

⊢ `Let`

$\mathcal{W}_{\mathrm{C}'_1}$ = $\mathcal{FB}$ [[L;M;S;T];[C_1]];

$\mathcal{W}_{\mathrm{C}'_2}$ = $\mathcal{FB}$ [[L;M;S;T];[C_2]];

$\mathcal{W}_{\mathrm{Q}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_1$];[$\mathrm{Q}_1$]];

$\mathcal{W}_{\mathrm{U}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_1$];[$\mathrm{Q}_2$]];[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_3$]];[$\mathrm{U}_1$]];

$\mathcal{W}_{\mathrm{Z}'_2}$ = $\mathcal{FB}_{\mathcal{N}}$ [[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_1$];[$\mathrm{Q}_2$]];[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_3$]];[$\mathrm{U}_2$];[$\mathrm{Z}_2$]];

$\mathcal{W}_{\mathrm{V}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_1$];[$\mathrm{Q}_2$]];[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_3$]];[$\mathrm{U}_2$];[$\mathrm{Z}_1$];[$\mathrm{V}_1$]];

$\mathcal{W}_{\mathrm{V}'_2}$ = $\mathcal{FB}_{\mathcal{N}}$ [[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_1$];[$\mathrm{Q}_2$]];[$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_3$]];[$\mathrm{U}_2$];[$\mathrm{Z}_1$];[$\mathrm{V}_2$]];

$\mathcal{W}_{\mathrm{E}'_2}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_2$];[$\mathrm{E}_2$]];

$\mathcal{W}_{\mathrm{I}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_2$];[$\mathrm{E}_1$];[$\mathrm{I}_1$]];

$\mathcal{W}_{\mathrm{I}'_2}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{C}'_1}$;[$\mathrm{Y}_2$];[$\mathrm{E}_1$];[$\mathrm{I}_2$]];

$\mathcal{W}_{\mathrm{X}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{Q}'_1}$;$\mathcal{W}_{\mathrm{U}'_1}$;$\mathcal{W}_{\mathrm{V}'_1}$;$\mathcal{W}_{\mathrm{I}'_1}$;[$\mathrm{X}_1$]];

$\mathcal{W}_{\mathrm{W}'_1}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{Q}'_1}$;$\mathcal{W}_{\mathrm{U}'_1}$;$\mathcal{W}_{\mathrm{V}'_1}$;$\mathcal{W}_{\mathrm{I}'_1}$;[$\mathrm{X}_2$];[$\mathrm{W}_1$]];

$\mathcal{W}_{\mathrm{W}'_2}$ = $\mathcal{FB}_{\mathcal{N}}$ [$\mathcal{W}_{\mathrm{Q}'_1}$;$\mathcal{W}_{\mathrm{U}'_1}$;$\mathcal{W}_{\mathrm{V}'_1}$;$\mathcal{W}_{\mathrm{I}'_1}$;[$\mathrm{X}_2$];[$\mathrm{W}_2$]];

$\mathrm{L}_{\mathrm{IEs}}$ = [L ↓ ; M ↓; S ↓; T ↓]

$\mathrm{L}_{\mathrm{States}}$ = [[C_1 ↑; C_2 ↓]; [Y_1 ↑; Y_2 ↓; ; Y_3 ↓]; [Q_1 ↑; Q_2 ↓];

[U_1 ↑; U_2 ↓]; [Z_1 ↑; Z_2 ↓; [V_1 ↑; V_2 ↓]; [E_1 ↑; E_2 ↓];

[I_1 ↑; I_2 ↓]; [X_1 ↑; X_2 ↓]; [W_1 ↑; W_2 ↓]]

`in` `OUTCOME_CLASS_I_BWR` $\mathrm{L}_{\mathrm{IEs}}$ $\mathrm{L}_{\mathrm{States}}$ = $\mathcal{FB}_{ET}$ ($\mathcal{FB}^{\mathcal{N}}_{ET}$ [$\mathcal{W}_{\mathrm{V}'_2}$;$\mathcal{W}_{\mathrm{Z}'_2}$])

$$\begin{aligned}
&\texttt{OUTCOME\_CLASS\_II\_BWR}\ \mathrm{L}_{\mathrm{IEs}}\ \mathrm{L}_{\mathrm{States}} = \mathcal{FB}_{ET}\ (\mathcal{W}_{\mathrm{W}'_2})\\
&\texttt{OUTCOME\_CLASS\_III\_BWR}\ \mathrm{L}_{\mathrm{IEs}}\ \mathrm{L}_{\mathrm{States}} = \mathcal{FB}_{ET}\ (\mathcal{FB}^{\mathcal{N}}_{ET}\ [\mathcal{W}_{\mathrm{E}'_2};\mathcal{W}_{\mathrm{I}'_2}])\\
&\texttt{OUTCOME\_CLASS\_IV\_BWR}\ \mathrm{L}_{\mathrm{IEs}}\ \mathrm{L}_{\mathrm{States}} = \mathcal{FB}_{ET}\ (\mathcal{W}_{\mathrm{C}'_2})\\
&\texttt{OUTCOME\_SUCCESS\_BWR}\ \mathrm{L}_{\mathrm{IEs}}\ \mathrm{L}_{\mathrm{States}} = \mathcal{FB}_{ET}\ (\mathcal{FB}^{\mathcal{N}}_{ET}\ [\mathcal{W}_{\mathrm{X}'_1};\mathcal{W}_{\mathrm{W}'_1}])
\end{aligned}$$

where the failure function ↓ or Cumulative Distribution Function (CDF) takes a component $\mathcal{X}$ and returns its probability of failure less than or equal to certain time t, i.e., $\mathcal{X} \leq\ t$, as described in Section 2.4, while the success distribution function ↑ is the complement of the function ↓ and returns its probability of success greater than a certain time t,, i.e, $\mathcal{X}\ >\ t$.

6.3.2 Formal Safety Classes Assessment

Using our proposed ET and FBD probabilistic theorems, we can easily generate and verify the probabilistic expression at the subsystem-level for any of the BWR safety outcome classes that could occur in the nuclear power plant. We assume that ↓ and ↑ events of all components within the nuclear power plant are continuous exponentially distributed (see Section 2.4). Therefore, we can verify the probabilistic expressions of all outcome classes *CLASS-II*, *CLASS-III*, *CLASS-I*, *CLASS-IV* and *SUCCESS* at the subsystem-level for the nuclear power plant, respectively, in HOL4 as follows:

Theorem 6.7. *Containment Failing when BWR Core Melts*

$\vdash\ \Omega^{\mathcal{N}}_{C}\ \texttt{[L;M;S;T]}\ \Rightarrow$

$\texttt{prob p (OUTCOME\_CLASS\_II\_BWR}\ \mathrm{L}_{\mathrm{IEs}}\ \mathrm{L}_{\mathrm{States}}\texttt{) =}$

$(1-\mathrm{e}^{(-\lambda_L t)})\ \times\ \mathrm{e}^{(-\lambda_C t)}\ \times\ \mathrm{e}^{(-\lambda_{Y2} t)}\ \times\ \mathrm{e}^{(-\lambda_{Y3} t)}\ \times\ \mathrm{e}^{(-\lambda_Q t)}\ \times\ (1-\mathrm{e}^{(-\lambda_X t)})\ \times$

$(1-\mathrm{e}^{(-\lambda_W t)})\ \texttt{+}\ (1-\mathrm{e}^{(-\lambda_M t)})\ \times\ \mathrm{e}^{(-\lambda_C t)}\ \times\ \mathrm{e}^{(-\lambda_{Y2} t)}\ \times\ \mathrm{e}^{(-\lambda_{Y3} t)}\ \times\ \mathrm{e}^{(-\lambda_Q t)}\ \times$

$(1-\mathrm{e}^{(-\lambda_X t)})\ \times\ (1-\mathrm{e}^{(-\lambda_W t)})\ \texttt{+}\ (1-\mathrm{e}^{(-\lambda_S t)})\ \times\ \mathrm{e}^{(-\lambda_C t)}\ \times\ \mathrm{e}^{(-\lambda_{Y2} t)}\ \times\ \mathrm{e}^{(-\lambda_{Y3} t)}\ \times$

$\mathrm{e}^{(-\lambda_Q t)}\ \times\ (1-\mathrm{e}^{(-\lambda_X t)})\ \times\ (1-\mathrm{e}^{(-\lambda_W t)})\ \texttt{+}\ (1-\mathrm{e}^{(-\lambda_T t)})\ \times\ \mathrm{e}^{(-\lambda_C t)}\ \times\ \mathrm{e}^{(-\lambda_{Y2} t)}\ \times$

$e^{(-\lambda_{Y3}t)} \times e^{(-\lambda_{Q}t)} \times (1 - e^{(-\lambda_{X}t)}) \times (1 - e^{(-\lambda_{W}t)}) + (1 - e^{(-\lambda_{L}t)}) \times e^{(-\lambda_{C}t)} \times$
$e^{(-\lambda_{Y2}t)} \times e^{(-\lambda_{Y3}t)} \times (1 - e^{(-\lambda_{Q}t)}) \times e^{(-\lambda_{U}t)} \times (1 - e^{(-\lambda_{X}t)}) \times \ldots + \ldots + \ldots +$
$(1 - e^{(-\lambda_{M}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y3}t)}) \times e^{(-\lambda_{U}t)} \times (1 - e^{(-\lambda_{X}t)}) \times$
$(1 - e^{(-\lambda_{W}t)}) + \ldots + (1 - e^{(-\lambda_{S}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y3}t)}) \times (1 - e^{(-\lambda_{U}t)}) \times$
$e^{(-\lambda_{Z}t)} \times e^{(-\lambda_{V}t)} \times \ldots + \ldots$

where the function $\Omega_C^{\mathcal{N}}$ ensures that all multi-state events are *distinct* (not similar to each other) and *disjoint* (cannot occur at the same time), as described in Definition 3.11.

Theorem 6.8. *Containment Intact when BWR Core Melts at High Internal Pressure*

$\vdash \Omega_C^{\mathcal{N}}$ `[L;M;S;T]` $\Rightarrow$
`prob p (OUTCOME_CLASS_III_BWR` L_{IEs} L_{States}`) =`
$(1 - e^{(-\lambda_{L}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y2}t)}) \times (1 - e^{(-\lambda_{E}t)}) + (1 - e^{(-\lambda_{M}t)}) \times$
$e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y2}t)}) \times (1 - e^{(-\lambda_{E}t)}) + (1 - e^{(-\lambda_{S}t)}) \times e^{(-\lambda_{C}t)} \times$
$(1 - e^{(-\lambda_{Y2}t)}) \times (1 - e^{(-\lambda_{E}t)}) + (1 - e^{(-\lambda_{T}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y2}t)}) \times$
$(1 - e^{(-\lambda_{E}t)}) + (1 - e^{(-\lambda_{L}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y2}t)}) \times e^{(-\lambda_{E}t)} \times (1 - e^{(-\lambda_{I}t)})$
$+ \ldots + \ldots + (1 - e^{(-\lambda_{T}t)}) \times e^{(-\lambda_{C}t)} \times (1 - e^{(-\lambda_{Y2}t)}) \times e^{(-\lambda_{E}t)} \times (1 - e^{(-\lambda_{I}t)})$

Theorem 6.9. *Containment Intact when BWR Core Melts at Low Pressure*

$\vdash \Omega_C^{\mathcal{N}}$ `[L;M;S;T]` $\Rightarrow$
`prob p (OUTCOME_CLASS_I_BWR` L_{IEs} L_{States}`) =`
$(1 - e^{(-\lambda_{L}t)}) \times (1 - e^{(-\lambda_{U}t)}) \times e^{(-\lambda_{Z}t)} \times (1 - e^{(-\lambda_{V}t)}) \times (1 - e^{(-\lambda_{Q}t)}) \times e^{(-\lambda_{Y2}t)}$
$\times \ldots + \ldots + (1 - e^{(-\lambda_{S}t)}) + \times (1 - e^{(-\lambda_{U}t)}) \times e^{(-\lambda_{Z}t)} \times (1 - e^{(-\lambda_{V}t)}) \times$
$(1 - e^{(-\lambda_{Q}t)}) \times e^{(-\lambda_{Y2}t)} \times \ldots + \ldots + \ldots + (1 - e^{(-\lambda_{M}t)}) \times (1 - e^{(-\lambda_{U}t)}) \times$
$e^{(-\lambda_{Z}t)} \times (1 - e^{(-\lambda_{V}t)}) \times (1 - e^{(-\lambda_{Y3}t)}) \times e^{(-\lambda_{C}t)} + \ldots + \ldots +$
$(1 - e^{(-\lambda_{T}t)}) \times (1 - e^{(-\lambda_{U}t)}) \times (1 - e^{(-\lambda_{Z}t)}) \times (1 - e^{(-\lambda_{Y3}t)}) \times e^{(-\lambda_{C}t)}$

Theorem 6.10. *BWR of Nuclear Power Plant Functions Correctly*

⊢ $\Omega_C^{\mathcal{N}}$ [L;M;S;T] ⇒

prob p (OUTCOME_SUCCESS_BWR $\mathrm{L}_{\mathrm{IEs}}$ $\mathrm{L}_{\mathrm{States}}$) =

1 -

$\Big((1-\mathrm{e}^{(-\lambda_L t)}) \times \mathrm{e}^{(-\lambda_C t)} \times \mathrm{e}^{(-\lambda_{Y2} t)} \times \mathrm{e}^{(-\lambda_{Y3} t)} \times \mathrm{e}^{(-\lambda_Q t)} \times (1-\mathrm{e}^{(-\lambda_X t)}) \times$

$(1-\mathrm{e}^{(-\lambda_W t)})$ + ...+ $(1-\mathrm{e}^{(-\lambda_M t)}) \times \mathrm{e}^{(-\lambda_C t)} \times \mathrm{e}^{(-\lambda_{Y2} t)} \times \mathrm{e}^{(-\lambda_{Y3} t)} \times$

$(1-\mathrm{e}^{(-\lambda_Q t)}) \times \mathrm{e}^{(-\lambda_U t)} \times (1-\mathrm{e}^{(-\lambda_X t)}) \times$ ...+ ...+ $(1-\mathrm{e}^{(-\lambda_S t)}) \times$

$\mathrm{e}^{(-\lambda_C t)} \times (1-\mathrm{e}^{(-\lambda_{Y3} t)}) \times \mathrm{e}^{(-\lambda_U t)} \times (1-\mathrm{e}^{(-\lambda_X t)}) \times (1-\mathrm{e}^{(-\lambda_W t)})$ + ...+

$(1-\mathrm{e}^{(-\lambda_L t)}) \times \mathrm{e}^{(-\lambda_C t)} \times (1-\mathrm{e}^{(-\lambda_{Y3} t)}) \times (1-\mathrm{e}^{(-\lambda_U t)}) \times \mathrm{e}^{(-\lambda_Z t)} \times \mathrm{e}^{(-\lambda_V t)} \times$

...+ ...+ ...+ $(1-\mathrm{e}^{(-\lambda_T t)}) \times \mathrm{e}^{(-\lambda_C t)} \times (1-\mathrm{e}^{(-\lambda_{Y2} t)}) \times (1-\mathrm{e}^{(-\lambda_E t)})$ + ...+

$(1-\mathrm{e}^{(-\lambda_M t)}) \times \mathrm{e}^{(-\lambda_C t)} \times (1-\mathrm{e}^{(-\lambda_{Y2} t)}) \times \mathrm{e}^{(-\lambda_E t)} \times (1-\mathrm{e}^{(-\lambda_I t)})$ + ...+ ...+

$(1-\mathrm{e}^{(-\lambda_L t)}) \times (1-\mathrm{e}^{(-\lambda_U t)}) \times \mathrm{e}^{(-\lambda_Z t)} \times (1-\mathrm{e}^{(-\lambda_V t)}) \times (1-\mathrm{e}^{(-\lambda_Q t)}) \times \mathrm{e}^{(-\lambda_{Y2} t)}$

$\times$ ...+ $(1-\mathrm{e}^{(-\lambda_S t)}) \times (1-\mathrm{e}^{(-\lambda_U t)}) \times \mathrm{e}^{(-\lambda_Z t)} \times (1-\mathrm{e}^{(-\lambda_V t)}) \times$ ...+ ...$\Big)$

The proof of the above-verified outcome classes expressions at the subsystem level was conducted using HOL4 tactics, such as EVAL_TAC, REAL_ARITH_TAC, DEP_REWRITE_TAC and POP_ORW [68] and using our developed HOL4 theories of ET and FBD. In order to validate our formally analysis results, we compare them with those obtained through: (1) manual paper-and-pencil analysis we conducted the following the FBD step-wise assessment proposed in [8]; (2) the commercial Isograph software for ET analysis [18]; and (3) MATLAB Monte-Carlo Simulation (MCS) following the random-based algorithm proposed in [26]. The MCS randomly predicts the real behavior patterns to estimate the average value of the various safety classes of complete/partial failure and reliability. On the other hand, Isograph does not analyze FBDs directly but rather ET models only, and hence the FBD of the BRW shown in Figure 6.8 had to be converted to a flat network of ETs. We consider the failure rates of the nuclear power plant components λ_L, λ_M, λ_S, λ_T, λ_C, λ_{Y2}, λ_{Y3},

Table 6.1: Safety Class Results of the Nuclear Power Plant

Types of Outcome Classes	Manual	Isograph	MATLAB	HOL4
OUTCOME CLASS I	0.01308	0.0131	0.0195	0.01308055491
OUTCOME CLASS II	0.05685	0.0569	0.0628	0.05684465922
OUTCOME CLASS III	0.02506	0.0251	0.0303	0.02506380531
OUTCOME CLASS IV	0.09554	0.0955	0.0896	0.09554010593
OUTCOME SUCCESS	0.80947	0.8095	0.7978	0.80947082132
CPU Time (Seconds)	–	35.461	112.928	8.123

λ_Q, λ_W, λ_U, λ_Z, λ_V, λ_E, λ_X, λ_I to be, respectively, 0.11, 0.12, 0.15, 0.16, 0.21, 0.15, 0.21, 0.57, 0.42, 0.23, 0.22, 0.16, 0.12, 0.57, and 0.46 per year [106]. We assume that the study is undertaken for one year, i.e., $t = 8760$ hours, Table 6.1 summarizes the results of the HOL4, manual, Isograph and MATLAB analyses for all BWR outcome classes. It can be noticed that the values of the safety classes obtained from our formal analysis are equivalent to the corresponding ones calculated using paper-and-pencil as well as Isograph software augmented with added accuracy in the computed values. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results at every run with errors between 3-8%. Moreover, the total CPU time for the above safety classes analysis using the HOL4 analysis is much faster than Isograph (4X) and MATLAB MCS (14X), as shown in Table 6.1. It required several days to model the nuclear power plant using the manual analysis while it was less consuming time (a matter of hours) using the Isograph software and MATLAB MCS, but the least modeling time is through using the HOL4 theorem prover.

6.4 Summary

In this chapter, we described the formalization of FBDs. We formalized the FBD basic constructor FB, which can be used to construct mathematically multi-level

FBDs. We used the ET theory in HOL4 to construct, reduce and partition ET models corresponding to FBs. We verified probabilistic theorems for different configurations of consecutive FBs. The HOL4 proofs required hierarchical levels of induction cases as well as the loading of our ET theory in HOL4 with all its parent theories, i.e., measure theory, probability theory, set theory, list theory, arithmetic theory, real theory and extended real theory. The proof-script of the formalization work presented in this chapter amounts to about 3,500 lines of HOL4 code [107]. Lastly, we conducted the formal FBD-based safety analysis of a nuclear power plant in HOL4, where we verified all possible safety classes of accident events that can occur in the nuclear reactor. We then validated our formal FBD probability risk assessment results with the corresponding ones obtained from MATLAB, Isograph and manual analysis.

During the system modeling and reliability analysis of safety-critical systems, industrial planners/designers usually require a computer-aided visualization facilities with graphical interfaces. Although the mathematical reliability analysis we conducted in HOL4 provides accurate results and consumes less CPU time, HOL4 as a software tool is unable to display the outcome graphs to users. Therefore, to overcome that particular limitation as well as to overcome the limitations of all existing available analysis methods, i.e., random-based MCS algorithms and error-prone manual reliability analysis, we propose in the next chapter a new software for FBD and ET modeling and analysis, called $\mathbb{FETMA}$, which is based on our definition of ET and FBD structures and the formally verified mathematical probabilistic formulations of ETs and FBDs in HOL4. $\mathbb{FETMA}$ provides pop-up input windows for all ET and FBD modeling functions, exactly as described in Chapters 3 and 6, which facilitates the input of the data from users and displays the FBD/ET graphs.

Chapter 7

$\mathbb{FETMA}$ Software for Reliability Analysis of Complex Systems

In this chapter, we develop of a *Functional Block Diagram and Event Tree Modeling and Analysis* software, called $\mathbb{FETMA}$, for industrial reliability and safety engineers as well as non-HOL4 users, which is based on our verified ET/FBD formalizations (c.f Chapters 3 and 6) and implemented in Python. We describe in detail the internal structure of and the algorithm of ET and FBD reliability analysis in the $\mathbb{FETMA}$ software. We apply $\mathbb{FETMA}$ on the ET reliability analysis of a power transmission distance protection and the FBD reliability analysis of an automated substation.

7.1 $\mathbb{FETMA}$ Software Internal Structure

$\mathbb{FETMA}$ is a software for functional block diagram and event tree modeling and analysis, which we implemented in Python programming language [54]. $\mathbb{FETMA}$ provides some new features not existing in any other commercial probabilistic risk assessment software, such as ITEM [21], SoHAR [19], ReliaSoft [20] and Isograph [18], including: (i) automatic construction of a complete complex, hierarchical and sequential ET models of complex systems; (ii) deletion/reduction of unnecessary ET nodes and branches; (iii) selection of ET paths that end with the same risk consequence based on reliability requirements of the given safety-critical system; and (iv) probabilistic evaluation of the occurrence of a certain event as well as evaluation of reliability indices. The internal structure of $\mathbb{FETMA}$ is depicted in Figure 7.1. The current version of $\mathbb{FETMA}$ provides two options of ET-based probabilistic risk assessment: (1) ET analysis for system-level reliability evaluation; and (2) FBD analysis for subsystem-level reliability evaluation. The structure of each selection in $\mathbb{FETMA}$ is described as:

ET Analysis consists of four main functions for ET step-wise analysis at the system level: (1) automatic generation of complete system ET model from a given list of system components and their operating states; (2) deletion of unnecessary nodes and branches to generate a reduced ET model; (3) partitioning of ET paths with respect to an event occurrence; and (4) probabilistic evaluation of all possible complete/partial failure and reliability events that can occur at system level.

FBD Analysis consists of 6 main functions for FBD step-wise analysis at the subsystem level: (1) construction of an FBD model for complex systems; (2) automatic construction of a complete ET model to each FB; (3) deletion/reduction of unnecessary ET nodes and branches for each FB; (4) composition of all ETs associated with their corresponding FBs together to form a complete subsystem-level hierarchical ET model; (5) partitioning of hierarchical ET paths; and (6) probabilistic evaluation of all possible failure/reliability events that can occur at subsystem level.

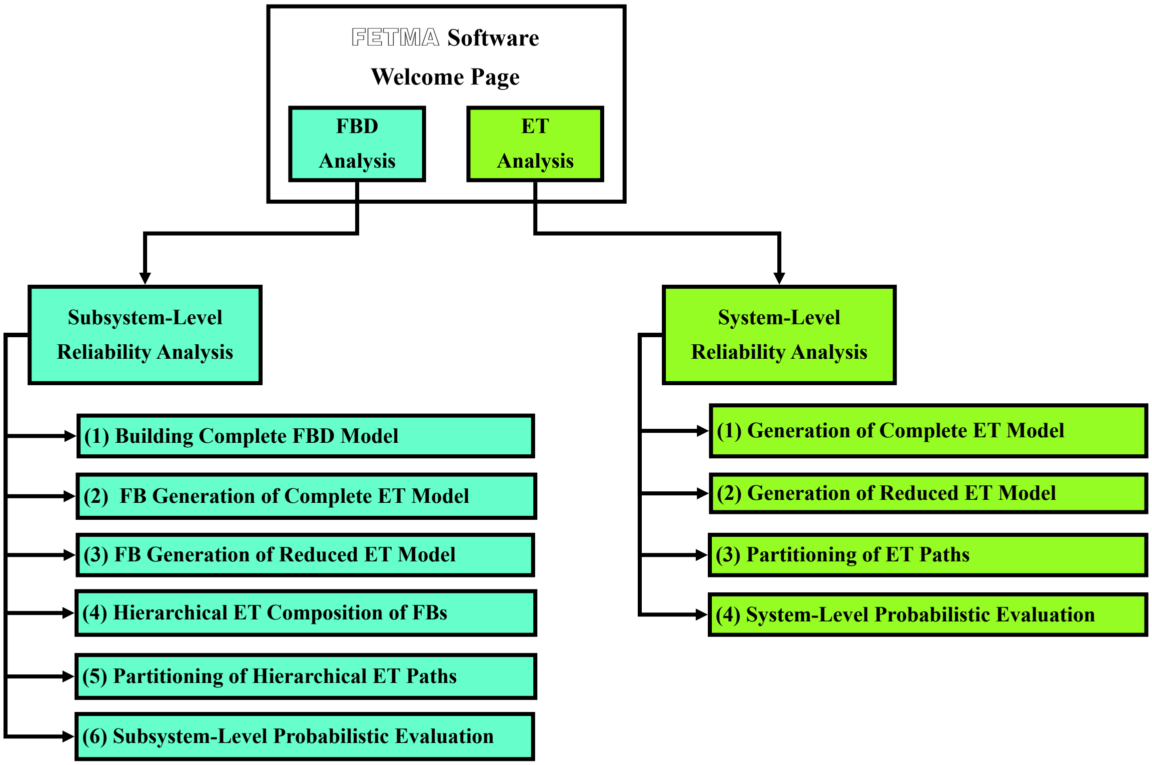

FETMA Software
Welcome Page
FBD
Analysis
ET
Analysis
Subsystem-Level
Reliability Analysis
System-Level
Reliability Analysis
(1) Building Complete FBD Model
(2) FB Generation of Complete ET Model
(3) FB Generation of Reduced ET Model
(4) Hierarchical ET Composition of FBs
(5) Partitioning of Hierarchical ET Paths
(6) Subsystem-Level Probabilistic Evaluation
(1) Generation of Complete ET Model
(2) Generation of Reduced ET Model
(3) Partitioning of ET Paths
(4) System-Level Probabilistic Evaluation

Figure 7.1: FETMA Software Internal Structure

7.2 ET Reliability Analysis in FETMA

The flowchart describing the FETMA software for system-level ETs modeling and analysis is depicted in Figure 7.2, which is based on the ET mathematical modeling functions and the verified ET probabilistic formulations presented in Chapter 3. The ET reliability analysis in FETMA consists of four main steps as follows: (1) identify the given system components and their operating states representing the behavior of the system, then automatically generate a complete ET model describing all system components states and also produce a complete outcome space with all possible scenarios of different levels of failure and success; (2) optionally, reduce manually some nodes/branches from the generated complete ET diagram by identifying the ET Complete Cylinders (CCs) and Conditional Events (CEs) (see *Step 2* of ET analysis in Section 2.1) to construct a smaller model exhibiting the exact behavior of the given system and reduce the number of possible test cases; (3) partition the ET paths according to the system reliability requirements; and (4) evaluate the probability of occurrence for certain events in the system after partitioning the ET paths. Also, Figure 7.2 shows the procedure of making a decision for redundancy of a critical component in a safety-critical system. If the level of the probabilistic risk analysis evaluated from the ET model is satisfied, then this component is duplicated. If the

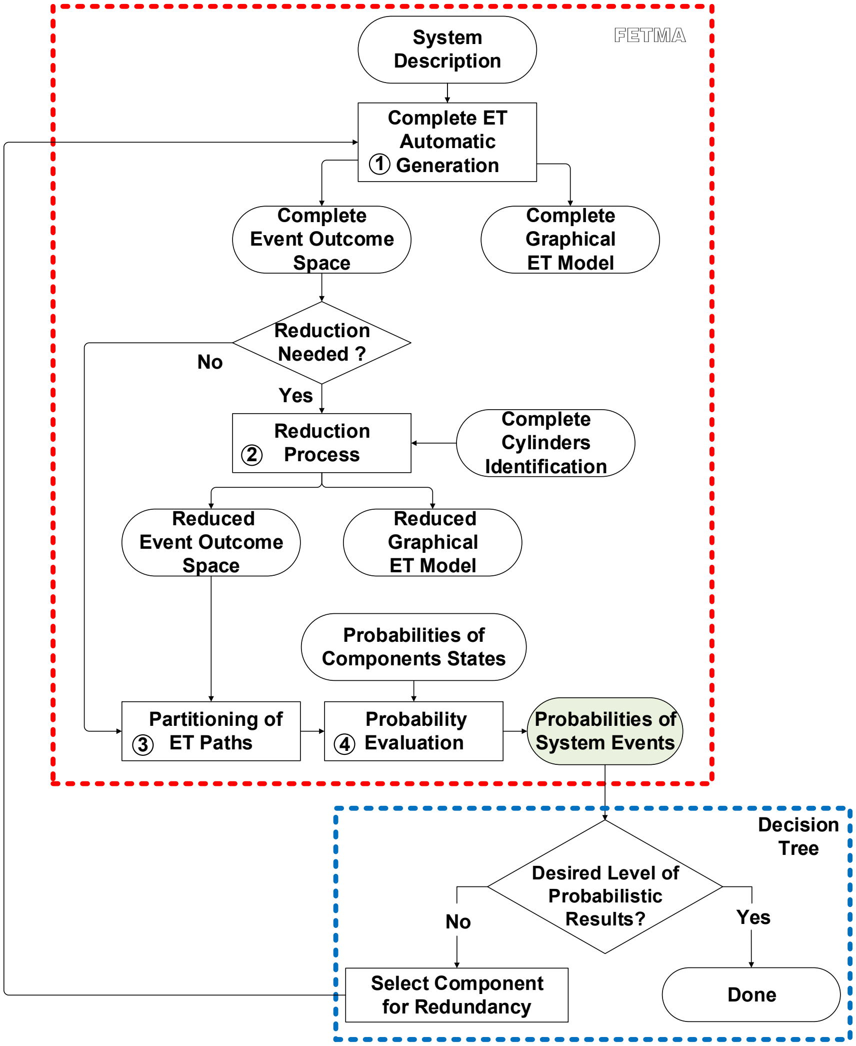

FETMA
System Description
Complete ET Automatic ① Generation
Complete Event Outcome Space
Complete Graphical ET Model
Reduction Needed ?
No
Yes
Reduction ② Process
Complete Cylinders Identification
Reduced Event Outcome Space
Reduced Graphical ET Model
Probabilities of Components States
Partitioning of ③ ET Paths
Probability ④ Evaluation
Probabilities of System Events
Decision Tree
Desired Level of Probabilistic Results?
No
Yes
Select Component for Redundancy
Done

Figure 7.2: ET Analysis Process in FETMA

results are not acceptable, then another critical component is selected for redundancy from the system and 𝔽𝔼𝕋𝕄𝔸 is used for the re-construction of the new ET model. The details of the 𝔽𝔼𝕋𝕄𝔸 functions that perform the above-mentioned operations are described in Algorithm 7.1. We provide pop-up input windows for each of these functions in order to facilitate the users interaction with the 𝔽𝔼𝕋𝕄𝔸 software. It can be noticed from Algorithm 7.1 that the reduction 𝔽𝔼𝕋𝕄𝔸 feature can be bypassed, in case the deletion of nodes or branches is not required.

In order to ensure that 𝔽𝔼𝕋𝕄𝔸 is capable of generating complex and scalable ETs for large number of components, where each component is represented by different multi-state model of complete/partial failure and reliability, we have implemented the steps of Algorithm 7.1 using the *PyGraphviz* Python package [108], which provides several methods for drawing complex graphs.

Algorithm 7.1. ET Analysis in 𝔽𝔼𝕋𝕄𝔸

```
procedure
S1: complete_gen
    Input: system name, system components, each system component states
    Output: complete ET model, complete event outcome space
If Reduction of ET model needed?
      then
      S2: reduction_process
          Input: CCs identification
          Output: reduced ET model, reduced event outcome space
S3: partitioning_paths
    Input: component event name(s), ET path number(s)
    Output: system events ET paths
S4: probability_eval
    Input: probabilities of components states
    Output: Occurrence probability of an event
end procedure
```

7.3 Application: Power Transmission Distance Protection

In this section, we use the ET Analysis feature of 𝔽𝔼𝕋𝕄𝔸 for the reliability analysis of distance protective fault tripping circuits in different zones of power transmission [109]. The distance protection fault Trip Circuit (TC) of power transmission systems is used to isolate faulty transmission lines to protect the rest of a power transmission grid from undesirable blackout situation for the whole grid, as shown in Figure 7.3 [110]. Consider a transmission line that consists of one Distance Relay (R) and one Current Transformer (CT), one Potential Transformer (PT), two Trip Circuits (TC) and two Circuit Breakers (CB), as shown in Figure 7.4 [109]. The figure depicts the strategy of *Zones of Protection*, which can be used to provide the level of transmission protection demanded by the utility. Protective distance relays keep the utility grids and the

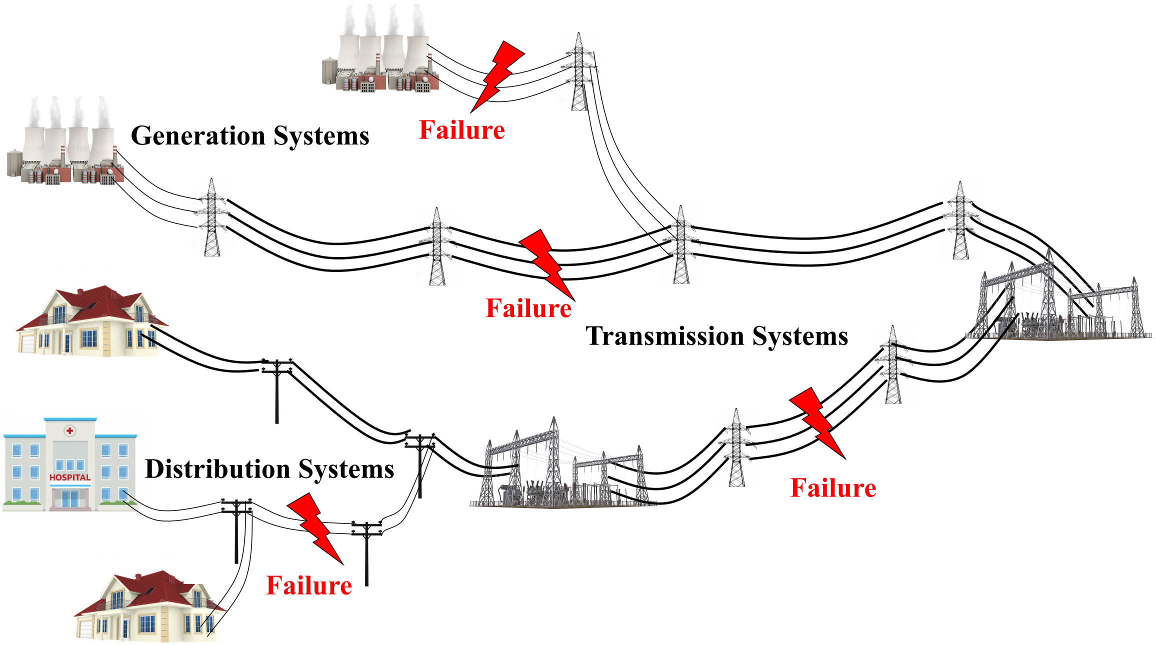


Figure 7.3: Cascading Failures of Power System Outage Zones

equipment safe from faults and system unbalances by dividing the grid into zones, where each relay has a unique protection scheme. Overlapping between different relay zones provides a backup utility protection. As shown in Figure 7.4, *Zone 1* protects the transmission line of instantaneous tripping in case of fault occurrence, while *Zone 2* and *Zone 3* provide fault isolation after a certain time of 0.2-0.5 and 0.8-2 seconds, respectively [111]. In this analysis, we focused on the reliability analysis of protective Zone 1. During normal operation, both circuit breakers CB_1 and CB_2 are in a closed position. If a fault occurs on the transmission line, the CT detects that there is a fault, then it energizes both TC_1 and TC_2. Each TC controls the circuit breakers CB_1 and CB_2 to open and thereupon isolates the faulty transmission line. Using the $\mathbb{FETMA}$ software, a detailed ET risk analysis of *Zone 1* for the protective distance protection can be done to obtain all possible consequence scenarios of complete/partial failure and reliability events as follows:

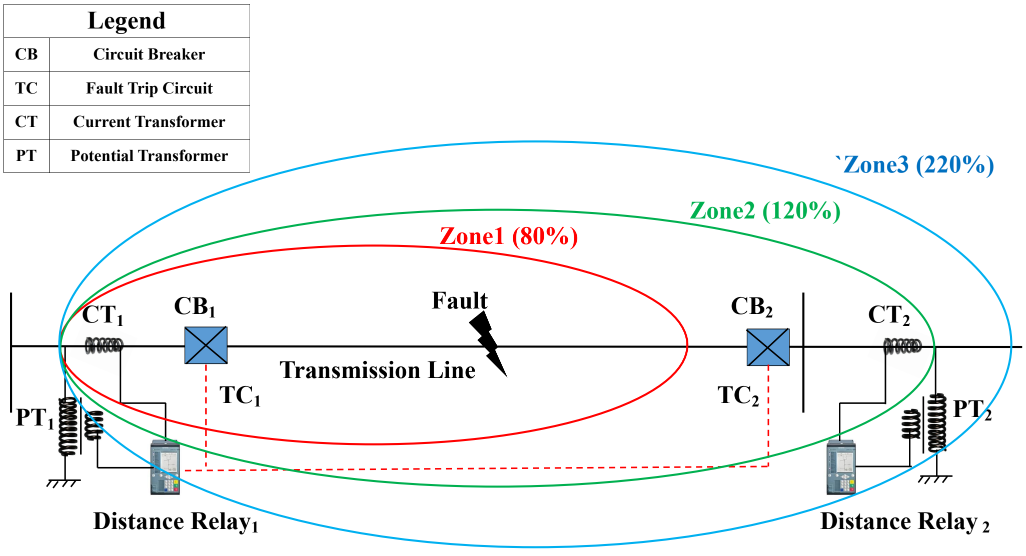
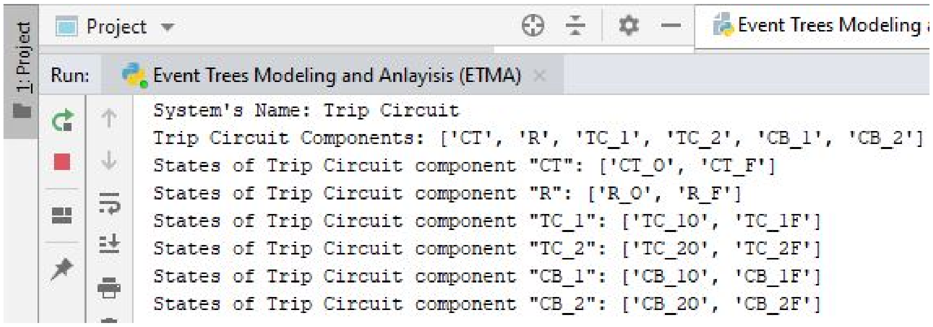


Figure 7.4: Single Line Diagram of Power Transmission Distance Protection

7.3.1 ET Analysis in FETMA

Step 1 (ET Generation):

We enter the details of the transmission protection components consisting of one CT, one R, two TCs (TC_1 and TC_2) and two CBs (CB_1 and CB_2) and each having two operational states, i.e., operating or failing, as shown in Figure 7.5. The entered details are sufficient for FETMA's function to automatically generate the complete graph ET model, see Figure 7.6 for a snapshot of a portion of the complete ET.



```
System's Name: Trip Circuit
Trip Circuit Components: ['CT', 'R', 'TC_1', 'TC_2', 'CB_1', 'CB_2']
States of Trip Circuit component "CT": ['CT_O', 'CT_F']
States of Trip Circuit component "R": ['R_O', 'R_F']
States of Trip Circuit component "TC_1": ['TC_1O', 'TC_1F']
States of Trip Circuit component "TC_2": ['TC_2O', 'TC_2F']
States of Trip Circuit component "CB_1": ['CB_1O', 'CB_1F']
States of Trip Circuit component "CB_2": ['CB_2O', 'CB_2F']
```

Figure 7.5: FETMA: Transmission Distance Protection Identification

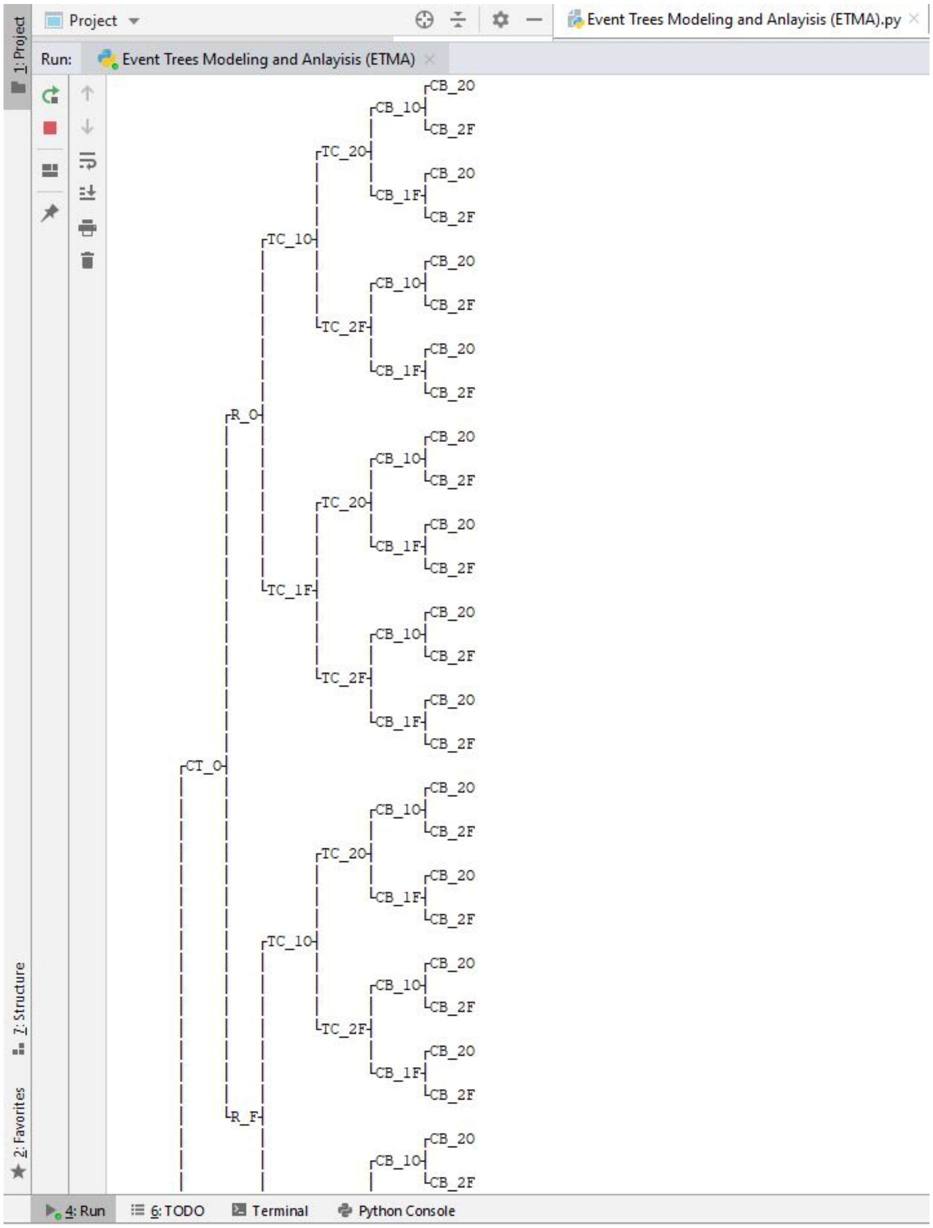
Step 2 (ET Reduction):

The second step is to select the nodes/branches of the protection scheme to be reduced, then FETMA generates the reduced ET model, as shown in Figure 7.7.

Step 3 (ET Partitioning):

Suppose, we are only focusing on the failure of CB_1, then paths 2, 3, and 5-10 are obtained. Similarly, different selection of paths can be obtained by observing the behavior of the transmission protection components as:

- Pr (CB_1 Only Fails) $= \sum Pr(2, 3, 5 - 10)$
- Pr (CB_1 Only Operates) $= \sum Pr(0, 1, 4)$
- Pr (CB_2 Only Fails) $= \sum Pr(1, 3 - 5, 7 - 10)$

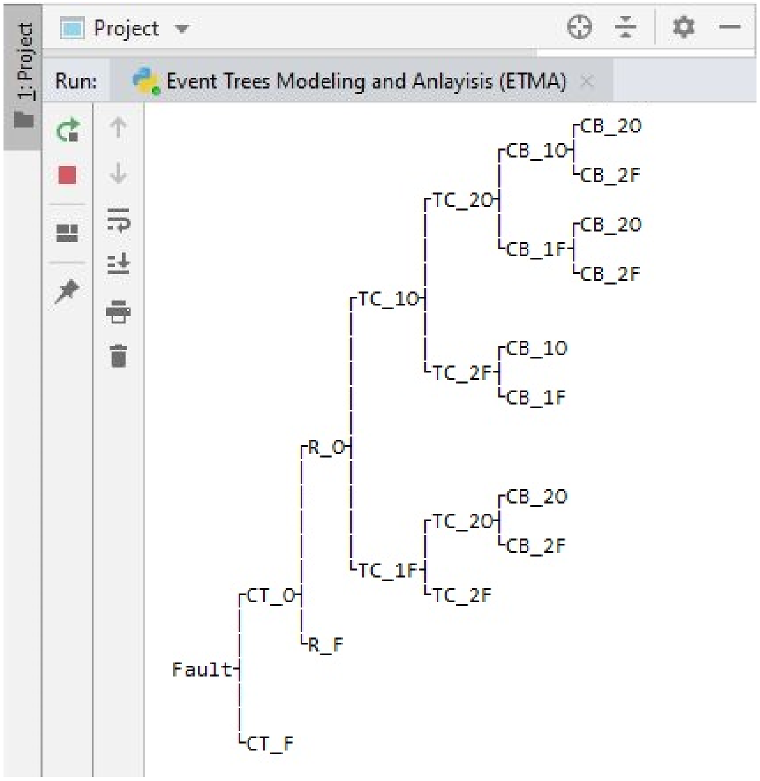

Project
Event Trees Modeling and Anlayisis (ETMA).py
Run:
Event Trees Modeling and Anlayisis (ETMA)
1: Project
7: Structure
2: Favorites
4: Run
6: TODO
Terminal
Python Console

```
                           ┌CB_2O
                     ┌CB_1O┤
                     │     └CB_2F
               ┌TC_2O┤
               │     │     ┌CB_2O
               │     └CB_1F┤
               │           └CB_2F
         ┌TC_1O┤
         │     │           ┌CB_2O
         │     │     ┌CB_1O┤
         │     │     │     └CB_2F
         │     └TC_2F┤
         │           │     ┌CB_2O
         │           └CB_1F┤
         │                 └CB_2F
     ┌R_O┤
     │   │                 ┌CB_2O
     │   │           ┌CB_1O┤
     │   │           │     └CB_2F
     │   │     ┌TC_2O┤
     │   │     │     │     ┌CB_2O
     │   │     │     └CB_1F┤
     │   │     │           └CB_2F
     │   └TC_1F┤
     │         │           ┌CB_2O
     │         │     ┌CB_1O┤
     │         │     │     └CB_2F
     │         └TC_2F┤
     │               │     ┌CB_2O
     │               └CB_1F┤
     │                     └CB_2F
┌CT_O┤
│    │                     ┌CB_2O
│    │               ┌CB_1O┤
│    │               │     └CB_2F
│    │         ┌TC_2O┤
│    │         │     │     ┌CB_2O
│    │         │     └CB_1F┤
│    │         │           └CB_2F
│    │   ┌TC_1O┤
│    │   │     │           ┌CB_2O
│    │   │     │     ┌CB_1O┤
│    │   │     │     │     └CB_2F
│    │   │     └TC_2F┤
│    │   │           │     ┌CB_2O
│    │   │           └CB_1F┤
│    │   │                 └CB_2F
│    └R_F┤
│        │                 ┌CB_2O
│        │           ┌CB_1O┤
│        │           │     └CB_2F
```

Figure 7.6: 𝔽𝔼𝕋𝕄𝔸: Transmission Distance Protection Complete ET Model

- Pr (CB_2 Only Operates) $= \sum Pr(0, 2, 6)$
- Pr (Both CB_1 and CB_2 Fail) $= \sum Pr(3, 5, 7 - 10)$
- Pr (Both CB_1 and CB_2 Operate) $= \sum Pr(0)$

To the best of our knowledge this feature is not available in any other ET software.



```
                                ┌CB_2O
                          ┌CB_1O┤
                          │     └CB_2F
                    ┌TC_2O┤
                    │     │     ┌CB_2O
                    │     └CB_1F┤
                    │           └CB_2F
              ┌TC_1O┤
              │     │
              │     │     ┌CB_1O
              │     └TC_2F┤
              │           └CB_1F
              │
          ┌R_O┤
          │   │
          │   │           ┌CB_2O
          │   │     ┌TC_2O┤
          │   │     │     └CB_2F
          │   └TC_1F┤
     ┌CT_O┤         └TC_2F
     │    │
     │    └R_F
Fault┤
     │
     │
     └CT_F
```

Figure 7.7: 𝔽𝔼𝕋𝕄𝔸: Transmission Distance Protection Reduced ET Model

Step 4 (ET Probabilistic Analysis):

We assign probability values to each state of the components, as shown in Table 7.1 [112]. Assuming that the times to failure of the transmission protection components are exponentially distribution, then the probabilities of the different transmission protection events, which are calculated using 𝔽𝔼𝕋𝕄𝔸 are as follows:

- Pr (Both CB_1 and CB_2 Fail) = 5.389960806400000%
- Pr (Both CB_1 and CB_2 Operate) = 82.429704806399980%
- Pr (CB_1 Only Fails) = 11.480127999999999%
- Pr (CB_1 Only Operates) = 88.519871999999980%
- Pr (CB_2 Only Fails) = 11.480127999999999%
- Pr (CB_2 Only Operates) = 88.519871999999980%

Table 7.1: Transmission Distance Protection Probability of Components States

Transmission Component	λ *(f/yr)*	Prob. of Failure (%)	Prob. of Success (%)
CT	0.06	CT_F (3%)	CT_O (97%)
R	0.04	R_F (2%)	R_O (98%)
TC_1	0.08	TC_{1F} (4%)	TC_{1O} (96%)
TC_2	0.08	TC_{2F} (4%)	TC_{2O} (96%)
CB_1	0.06	CB_{1F} (3%)	CB_{1O} (97%)
CB_2	0.06	CB_{2F} (3%)	CB_{2O} (97%)

It can be observed that the probability of both circuit breakers CB_1 and CB_2 failing is evaluated as 5.389960806400000%. If we want to decrease their probability to 2.5% or less (i.e., improving the probability of fault tripping in Zone 1 of the transmission protection system), then we may add redundancy to these components. However, in order to ensure that the redundancy to some critical-components are a correct decision, we need to conduct the decision redundancy analysis of the transmission distance protection components, which is presented in the next section.

7.3.2 Redundancy Analysis in $\mathbb{FETMA}$

A decision-tree describing the process of selecting the redundancy for critical transmission protection components is shown in Figure 7.8. First, we select CT only for redundancy (i.e., adding CT_2) assuming the same probability of failure and success of CT_1. If the probability of both circuit breakers CB_1 and CB_2 failing together, after re-evaluation in $\mathbb{FETMA}$, is equal to 2.5% or less as required, then this is a correct decision. If not, then we select the critical component R for redundancy. If we still do not achieve the desired level of probability, then we select both CT and R together. If the results are not acceptable, then we make a new component selection from the transmission protection system. Figure 7.9 shows the comparison among the old and

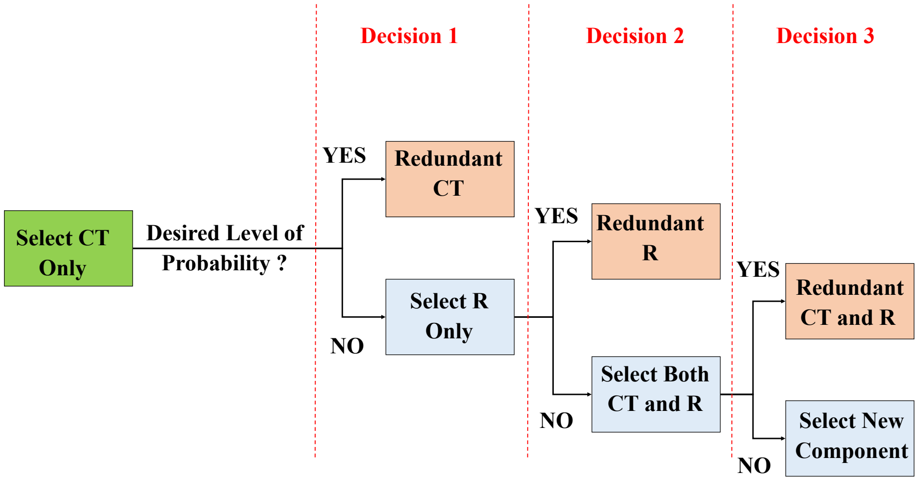


Figure 7.8: Decision Tree for the Transmission Protection Redundancy

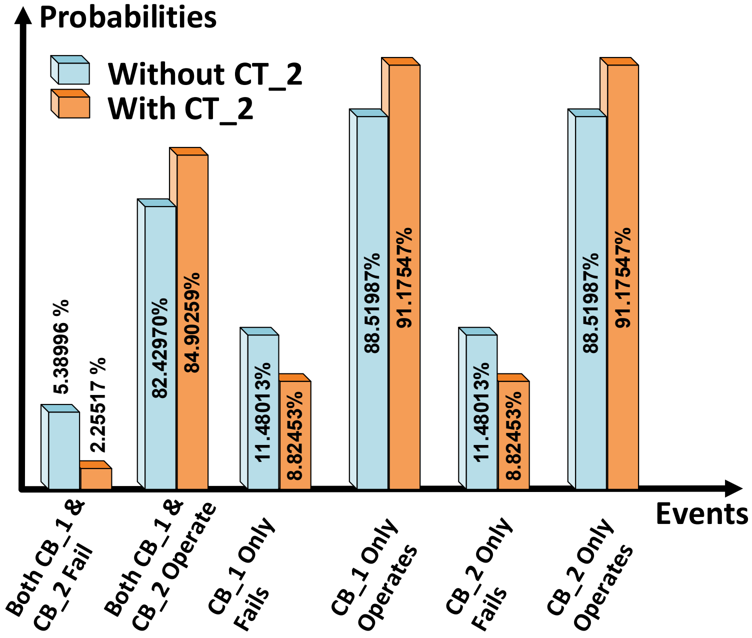


Figure 7.9: Transmission Protection Events Probabilities Evaluation

new probabilistic risk assessment values in a histogram plot using FETMA. It can be seen that the probability percentage of the circuit breakers CB_1 and CB_2 failing together is decreased from 5.38996% to 2.25517% by an amount of 3.13479%. Similarly, the proportion of the circuit breakers CB_1 and CB_2 succeeding together is also increased from 82.42970% to 84.90259% with an increment of 2.47289%.

To ensure the accuracy of the 𝔽𝔼𝕋𝕄𝔸 computation, we analyze the protection system without any redundancy in the critical components using the commercial Isograph software [18]. It is important to mention that, unlike 𝔽𝔼𝕋𝕄𝔸, Isograph requires from the users to manually draw the transmission protection actual ET model while 𝔽𝔼𝕋𝕄𝔸 automatically generates the ET model. The comparison in risk analysis of the protection system between 𝔽𝔼𝕋𝕄𝔸 and Isograph is presented in Table 7.2. It can be observed that the probabilities obtained from 𝔽𝔼𝕋𝕄𝔸 are equivalent to the corresponding ones calculated using Isograph. Moreover, the CPU time for the ET analysis in 𝔽𝔼𝕋𝕄𝔸 is much faster than Isograph, as shown in Table 7.3.

Table 7.2: Transmission Protection Comparison Between 𝔽𝔼𝕋𝕄𝔸 and Isograph

Transmission Protection Events	% Prob. from Isograph	% Prob. from 𝔽𝔼𝕋𝕄𝔸
Both CB_1 and CB_2 Fail	5.38996 %	5.389960806400000 %
Both CB_1 and CB_2 Operate	82.43 %	82.429704806399980 %
CB_1 Only Fails	11.48 %	11.480127999999999 %
CB_1 Only Operates	88.52 %	88.519871999999980 %
CB_2 Only Fails	11.48 %	11.480127999999999 %
CB_2 Only Operates	88.52 %	88.519871999999980 %

Table 7.3: 𝔽𝔼𝕋𝕄𝔸: Transmission Protection CPU time

Steps	CPU Time 𝔽𝔼𝕋𝕄𝔸 (*Seconds*)	CPU Time Isograph (*Seconds*)	*Steps*	CPU Time 𝔽𝔼𝕋𝕄𝔸 (*Seconds*)	CPU Time Isograph (*Seconds*)
Step 1	0.291600	NA	*Step* 3	0.000631	NA
Step 2	0.000162	NA	*Step* 4	0.004319	2.752

7.4 FBD Reliability Analysis in 𝔽𝔼𝕋𝕄𝔸

In this section, we describe the FBD reliability analysis option of the 𝔽𝔼𝕋𝕄𝔸 software, which allows planners/designers to perform the probabilistic reliability evaluation of safety-critical systems at the subsystem level. The flowchart describing the FBD modeling and analysis process in 𝔽𝔼𝕋𝕄𝔸 is depicted in Figure 7.10. The FBD reliability analysis in the 𝔽𝔼𝕋𝕄𝔸 software consists of the following six main steps:

1. Construction of the FBD for a given safety-critical system decomposed into hierarchical FBs corresponding to all subsystems.
2. Identifying for each subsystem FB its components and their operating states,

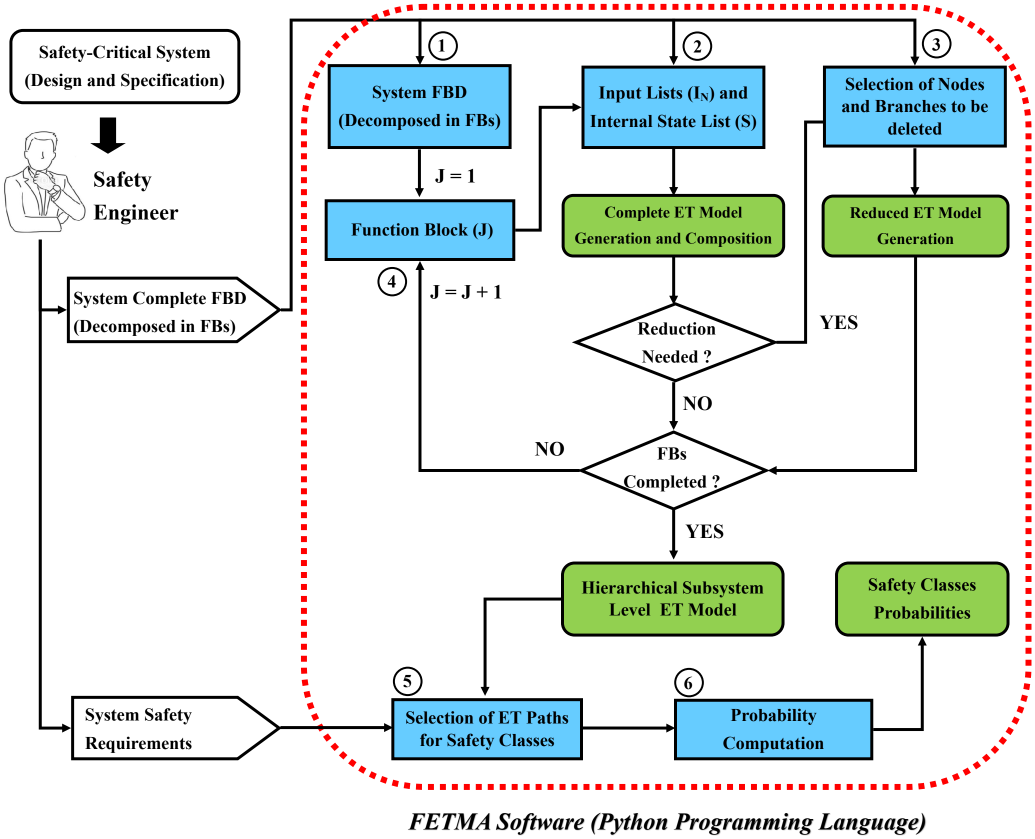


Figure 7.10: FBD Analysis Process in 𝔽𝔼𝕋𝕄𝔸

then automatically generate a complete ET graph describing all possible failure/success paths.

3. Selecting some nodes and branches from the generated complete complex ET model at the subsystem level to build a reduced ET graph.
4. Iterative composition of all subsystem ET models associated with all FBs together until a hierarchical subsystem-level ET structure is formed.
5. Selection of particular ET paths from the automatically generated hierarchical ET model for safety classes based on system safety requirements
6. Probabilistic evaluation of all safety classes of complete/partial failure and reliability events that can occur in the system.

Algorithm 7.2 describes the details of 𝔽𝔼𝕋𝕄𝔸 functions that perform the six FBD processes, i.e., FBD construction, ET generation, ET reduction, ET composition, ET partitioning, and probabilistic evaluation. We provide pop-up input windows for all of these functions in order to facilitate the industrial users interaction with 𝔽𝔼𝕋𝕄𝔸. First, a user has to input the hierarchical *multi-level* N FBs structure of the safety-critical system (S1), then 𝔽𝔼𝕋𝕄𝔸 takes the first FB corresponding to the first subsystem ($J = 1$) and asks the user to input the component names and their failure and reliability states (S2). Thereafter, 𝔽𝔼𝕋𝕄𝔸 automatically generates the complete ET model and asks if that ET model needs to be reduced or not, then repeats the same process for the next FB ($J = J + 1$) (S3). At this stage, 𝔽𝔼𝕋𝕄𝔸 connects/composes the new automatically generated ET model (J) with the previous subsystem ET model (J - 1) (S4). After composing all FBs of the safety-critical system, then the user selects the paths from the generated hierarchical ET model that end with the same risk consequence (S5). The last step is to evaluate the probability for all possible risk events that can occur in a critical-system at each subsystem level (S6).

Algorithm 7.2. FBD Analysis in $\mathbb{FETMA}$

```
procedure
S1: FBD_gen
  Input: hierarchical system N FBs
    J = 1
    while (J ≤ N)
      S2: complete_gen
         Input: FB (J) inputs and internal states
         Output: subsystem (J) $\mathrm{ET}_{\mathrm{Complete}}$, $\mathcal{W}_{\mathrm{Complete}}$ (J)
      If Reduction of ET model needed?
      then
      S3: reduction_process
         Input: select nodes and branches
         Output: subsystem (J) $\mathrm{ET}_{\mathrm{Reduced}}$, $\mathcal{W}_{\mathrm{Reduced}}$ (J)
      S4: composition_process
         Input: $\mathcal{W}_{\mathrm{Complete}}$ (J) or $\mathcal{W}_{\mathrm{Reduced}}$ (J)
         Output: $\mathcal{W}$ (J) $\bigotimes$ $\mathcal{W}$ (J - 1)
    J = J + 1
  Output: subsystem-level ET graph, subsystem-level outcome space $\mathcal{W}$
S5: partitioning_paths
    Input: system safety requirements, select ET path(s)
    Output: system accident events ET paths
S6: probability_eval
    Input: probabilities of all components states
    Output: occurrence probability of an event
end procedure
```

7.5 Application: Smart Automated Substation

An electrical substation is a substantial part of Smart Grids (SG) [57], which transforms voltage from high to low or the reverse, where the electric power may pass through several substations at different voltage levels. Smart Automated Substations (SAS) are constructed based on advanced monitoring infrastructure, control and protection devices, to operate as joint and multitask networks [113]. For that reason, substation power equipment, such as Automatic Circuit Reclosers (ACR), Circuit Breakers (CB), Disconnecting Switches (DS), Current Transformers (CT), and Potential Transformers (PT), have been equipped with digital transceivers, making the control and automation through the SAS more achievable [114]. Figure 7.11 [115] depicts such a smart automated substation, which consists of three main hierarchical levels, *Process*, *Bay* and *Station*, as follows [116]:

1. *Process Level*: It includes Merging Units (MU) to collect periodically the analog data from sensors and indicators of switchgear equipment, such as CTs, PTs and CBs, through copper wiring. Then MUs transit all equipment data to the upper process bus through a digital network.
2. *Bay Level*: It consists of Intelligent Electronic Devices (IED), such as Bay Control Units (BCU), Bay Protection Units (BPU), Phasor Measurement Units (PMU), and Measuring Centers (MC), which are energized by a DC Power Supply (PS). They are responsible for gathering all real-time data in each bay and send them to the higher level via communication Ethernet (EI) devices, such as Ethernet Switches (ESW). There exist five different topologies for IED connection configuration, such as simple cascading, redundant cascading, ring, star and hybrid. In this study, we will use a *simple cascade* for connecting IEDs.
3. *Station Level*: It integrates the Supervisory Control and Data Acquisition (SCADA) center to perform remote monitoring and controlling of the SAS system. The SCADA system uses Industrial Personal Computer (IPC) and Human Machine Interface (HMI) to display the real-time process data. SCADA also restores all collected data from the Bay Level in a main Server (Hot) as well as a backup mirrored Server (Standby) to prevent the cause of permanent data loss of the SAS. Moreover, the SCADA system utilizes a Gateway (GW) to provide a connection to upper-level Network Control Center (NCC) in the SG.

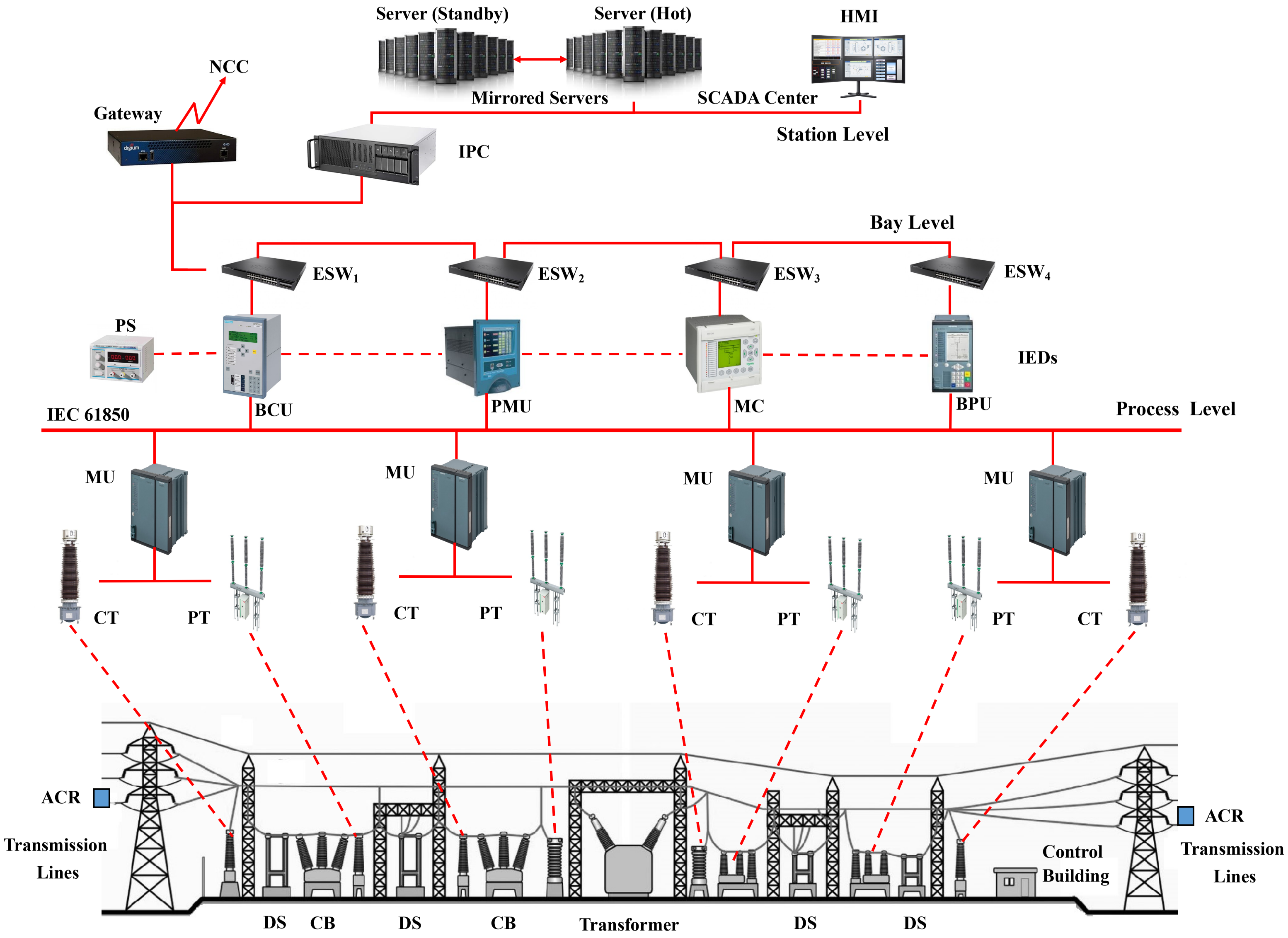


Figure 7.11: Automated Substation of a Smart Power Grid System

We now apply the 𝔽𝔼𝕋𝕄𝔸 to perform the FBD six step-analysis of the SAS system (see Figure 7.11) and determine the probabilistic risk assessment of all possible safety classes of complete/partial failure and reliability at the subsystem level.

7.5.1 FBD Analysis in 𝔽𝔼𝕋𝕄𝔸

Step 1 (FBD Construction):

We enter the FBD multiple-level model of the SAS system, as shown in Figure 7.12. The SAS system can be subjected to sudden Initial Events (IE) [117]: (a) T: Transient failures; (b) SP: Semi-Permanent failures; and (c) P: Permanent failures, where these failures could be any of commonly Transmission Line (TL) faults, such as Line-to-ground (L-G), Line-to-line (L-L), Three-phase-fault (L-L-L), and Three-line-to-earth (L-L-L-G), that must be isolated. Based on these IEs, there are three SAS safety classes [118] that can occur, as shown in Figure 7.12: (1) $SUCCESS$: all the required functions are available and the isolation is completed successfully; (2) *CLASS I (Manageable Failure)*: some of the required functions are not available, however, there is still a possibility to complete the isolation; and lastly (3) *CLASS II (Complete Failure)*: the completion of the action is impossible due to a failure of necessary functions. Each FB of the SAS can be assigned with a *multi-state* model for safety analysis (see Figure 3.1). We assume that each FB has two possible safety states only (correct functioning C_1 and failure operation C_2). For instance, FB$_{11}$ has two operating states: (a) ACR_1: Safety reclosure works correctly for fault isolation; and (b) ACR_2: Safety reclosure fails to open. Using 𝔽𝔼𝕋𝕄𝔸 input pop-up windows, we identify the failure/success states of all SAS subsystem-level components, i.e., *Process level* (ACR, CB$_1$, CB$_2$, CT$_1$, PT$_1$, MU$_1$, CT$_2$, PT$_2$, MU$_2$, CT$_3$, PT$_3$, MU$_3$, CT$_4$, PT$_4$, MU$_4$), *Bay level* (PS, BCU, ESW$_1$, PMU, ESW$_2$, MC, ESW$_3$, BPU, ESW$_4$, EI) and *Station level*

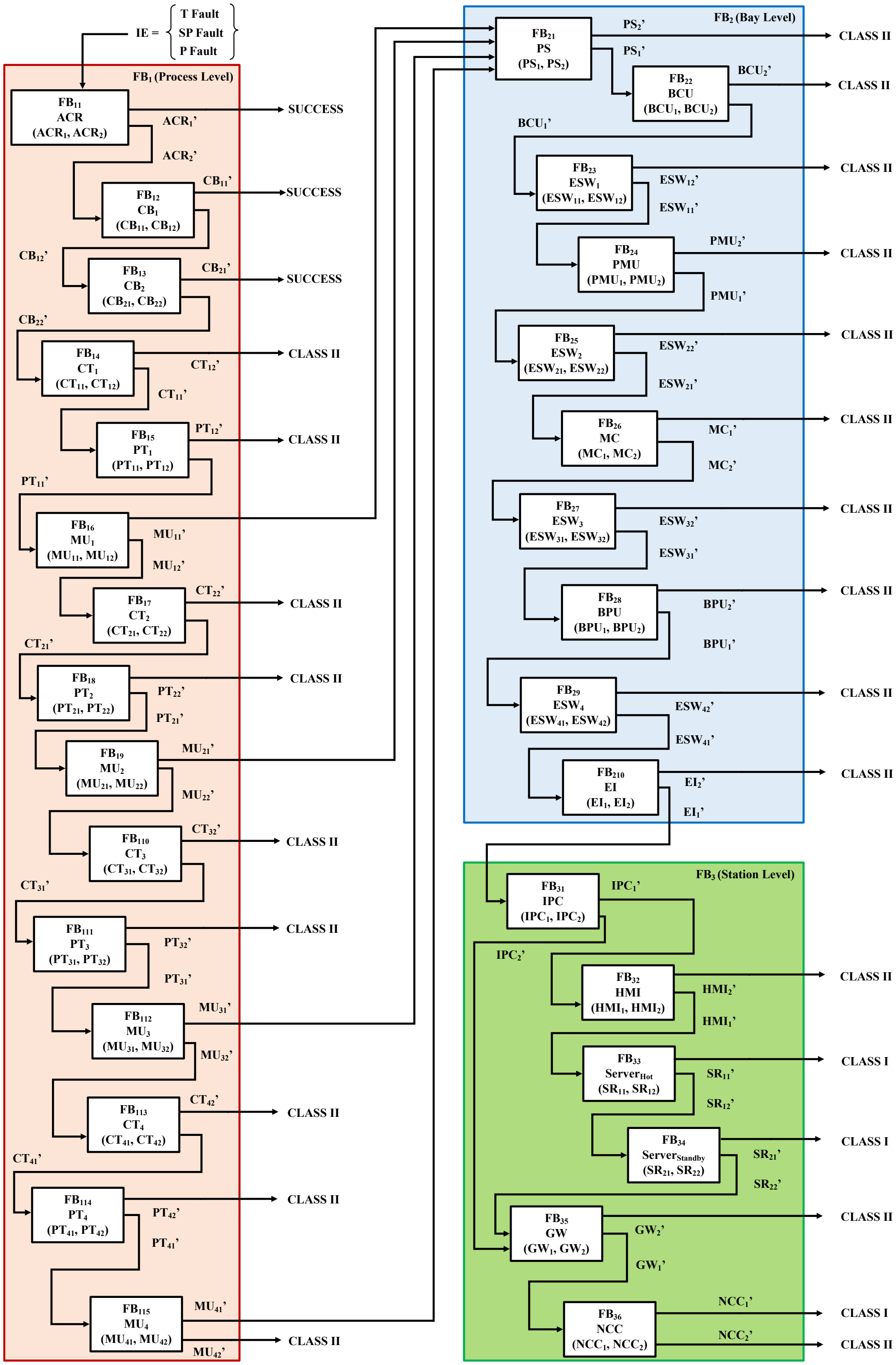
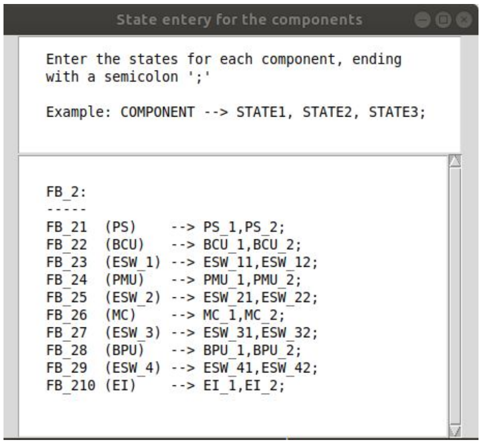

IE =
T Fault
SP Fault
P Fault
FB$_1$ (Process Level)
FB$_{11}$ ACR (ACR$_1$, ACR$_2$)
ACR$_1$'
SUCCESS
ACR$_2$'
FB$_{12}$ CB$_1$ (CB$_{11}$, CB$_{12}$)
CB$_{11}$'
SUCCESS
CB$_{12}$'
FB$_{13}$ CB$_2$ (CB$_{21}$, CB$_{22}$)
CB$_{21}$'
SUCCESS
CB$_{22}$'
FB$_{14}$ CT$_1$ (CT$_{11}$, CT$_{12}$)
CLASS II
CT$_{12}$'
CT$_{11}$'
FB$_{15}$ PT$_1$ (PT$_{11}$, PT$_{12}$)
PT$_{12}$'
CLASS II
PT$_{11}$'
FB$_{16}$ MU$_1$ (MU$_{11}$, MU$_{12}$)
MU$_{11}$'
MU$_{12}$'
FB$_{17}$ CT$_2$ (CT$_{21}$, CT$_{22}$)
CT$_{22}$'
CLASS II
CT$_{21}$'
FB$_{18}$ PT$_2$ (PT$_{21}$, PT$_{22}$)
CLASS II
PT$_{22}$'
PT$_{21}$'
FB$_{19}$ MU$_2$ (MU$_{21}$, MU$_{22}$)
MU$_{21}$'
MU$_{22}$'
FB$_{110}$ CT$_3$ (CT$_{31}$, CT$_{32}$)
CT$_{32}$'
CLASS II
CT$_{31}$'
FB$_{111}$ PT$_3$ (PT$_{31}$, PT$_{32}$)
CLASS II
PT$_{32}$'
PT$_{31}$'
FB$_{112}$ MU$_3$ (MU$_{31}$, MU$_{32}$)
MU$_{31}$'
MU$_{32}$'
FB$_{113}$ CT$_4$ (CT$_{41}$, CT$_{42}$)
CT$_{42}$'
CLASS II
CT$_{41}$'
FB$_{114}$ PT$_4$ (PT$_{41}$, PT$_{42}$)
CLASS II
PT$_{42}$'
PT$_{41}$'
FB$_{115}$ MU$_4$ (MU$_{41}$, MU$_{42}$)
MU$_{41}$'
CLASS II
MU$_{42}$'
FB$_2$ (Bay Level)
FB$_{21}$ PS (PS$_1$, PS$_2$)
PS$_2$'
CLASS II
PS$_1$'
FB$_{22}$ BCU (BCU$_1$, BCU$_2$)
BCU$_2$'
CLASS II
BCU$_1$'
FB$_{23}$ ESW$_1$ (ESW$_{11}$, ESW$_{12}$)
CLASS II
ESW$_{12}$'
ESW$_{11}$'
FB$_{24}$ PMU (PMU$_1$, PMU$_2$)
PMU$_2$'
CLASS II
PMU$_1$'
FB$_{25}$ ESW$_2$ (ESW$_{21}$, ESW$_{22}$)
CLASS II
ESW$_{22}$'
ESW$_{21}$'
FB$_{26}$ MC (MC$_1$, MC$_2$)
CLASS II
MC$_1$'
MC$_2$'
FB$_{27}$ ESW$_3$ (ESW$_{31}$, ESW$_{32}$)
CLASS II
ESW$_{32}$'
ESW$_{31}$'
FB$_{28}$ BPU (BPU$_1$, BPU$_2$)
CLASS II
BPU$_2$'
BPU$_1$'
FB$_{29}$ ESW$_4$ (ESW$_{41}$, ESW$_{42}$)
CLASS II
ESW$_{42}$'
ESW$_{41}$'
FB$_{210}$ EI (EI$_1$, EI$_2$)
CLASS II
EI$_2$'
EI$_1$'
FB$_3$ (Station Level)
FB$_{31}$ IPC (IPC$_1$, IPC$_2$)
IPC$_1$'
IPC$_2$'
FB$_{32}$ HMI (HMI$_1$, HMI$_2$)
CLASS II
HMI$_2$'
HMI$_1$'
FB$_{33}$ Server$_{Hot}$ (SR$_{11}$, SR$_{12}$)
CLASS I
SR$_{11}$'
SR$_{12}$'
FB$_{34}$ Server$_{Standby}$ (SR$_{21}$, SR$_{22}$)
CLASS I
SR$_{21}$'
SR$_{22}$'
FB$_{35}$ GW (GW$_1$, GW$_2$)
CLASS II
GW$_2$'
GW$_1$'
FB$_{36}$ NCC (NCC$_1$, NCC$_2$)
NCC$_1$'
CLASS I
NCC$_2$'
CLASS II

Figure 7.12: FBD Multiple-Levels Decomposition of the SAS System

(IPC, HMI, Server$_{Hot}$, Server$_{Standby}$, GW, NCC), as shown in Figure 7.13(a) and Figure 7.13(b), for bay and station levels, respectively.

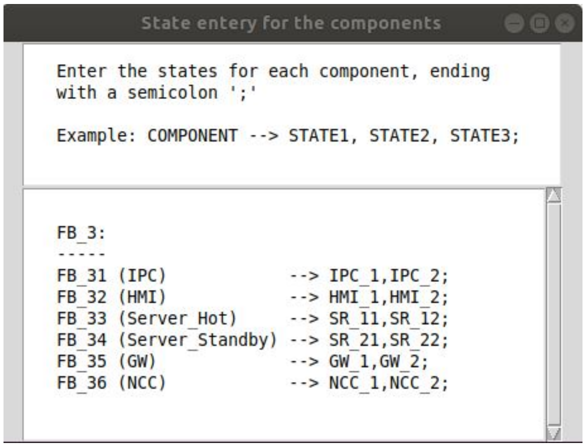


```
Enter the states for each component, ending
with a semicolon ';'

Example: COMPONENT --> STATE1, STATE2, STATE3;

FB_2:
-----
FB_21  (PS)    --> PS_1,PS_2;
FB_22  (BCU)   --> BCU_1,BCU_2;
FB_23  (ESW_1) --> ESW_11,ESW_12;
FB_24  (PMU)   --> PMU_1,PMU_2;
FB_25  (ESW_2) --> ESW_21,ESW_22;
FB_26  (MC)    --> MC_1,MC_2;
FB_27  (ESW_3) --> ESW_31,ESW_32;
FB_28  (BPU)   --> BPU_1,BPU_2;
FB_29  (ESW_4) --> ESW_41,ESW_42;
FB_210 (EI)    --> EI_1,EI_2;
```

(a) $\mathbb{FETMA}$: Bay Level Identification



```
Enter the states for each component, ending
with a semicolon ';'

Example: COMPONENT --> STATE1, STATE2, STATE3;

FB_3:
-----
FB_31 (IPC)            --> IPC_1,IPC_2;
FB_32 (HMI)            --> HMI_1,HMI_2;
FB_33 (Server_Hot)     --> SR_11,SR_12;
FB_34 (Server_Standby) --> SR_21,SR_22;
FB_35 (GW)             --> GW_1,GW_2;
FB_36 (NCC)            --> NCC_1,NCC_2;
```

(b) $\mathbb{FETMA}$: Station Level Identification

Figure 7.13: $\mathbb{FETMA}$ Software: Smart Automated Substation Identification

Steps 2-4 (Subsystem-Level ET Generation):

We now generate automatically a complete ET graph for each subsystem FB of the SAS system of Figure 7.12, then utilize the ET reduction feature in $\mathbb{FETMA}$ to generate a reduced ET model. After that, we use the composition feature of $\mathbb{FETMA}$ to generate a hierarchically composed ET model with all actual complete/partial failure and success scenarios at the subsystem-level (88 ET paths from 0 to 87 out of the complete 2^{31} test cases), as shown in Figure 7.14. To the best of our knowledge this ET composition feature is not found in any other ET analysis software.

Steps 5 (ET Partitioning):

The partitioning process of the generated event outcome space $\mathcal{W}_{SAS}$ is essential as substation safety analysts are interested in evaluating the probabilities of the occurrence of certain complete/partial failure and reliability events. Therefore, we can obtain different collections of subsystem-level ET paths, as shown in Figure 7.14, by observing the actual behavior of the SAS system as follows:

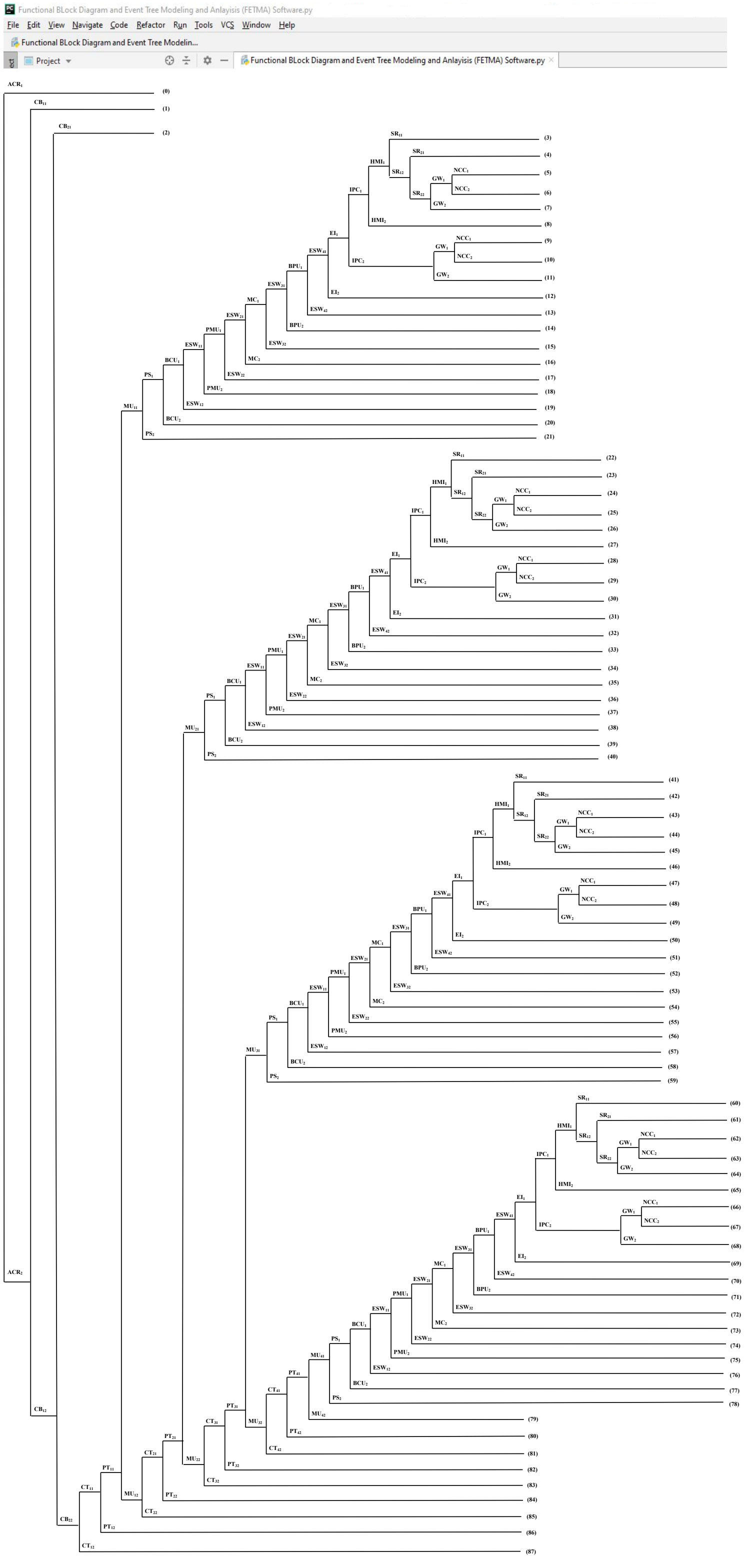


Figure 7.14: 𝔽𝔼𝕋𝕄𝔸: Reduced Subsystem-Level Event Tree of the SAS System

- $\text{SAS}_{SUCCESS}$ (Complete Success) $= \sum \text{ET}_{\text{Paths}}(0, 1, 2)$
- SAS_{CLASS_I} (Manageable Failure) $=$ $\sum \text{ET}_{\text{Paths}}(3-5, 9, 22-24, 28, 41-43, 47, 60-62, 66)$
- $\text{SAS}_{CLASS_{II}}$ (Complete Failure) $=$ $\sum \text{ET}_{\text{Paths}}(6-8, 10-21, 25-27, 29-40, 44-46, 48-59, 63-65, 67-87)$

7.5.2 Safety Classes Assessment in $\mathbb{FETMA}$

We can evaluate the probabilities for any of the SAS safety classes that can occur at the subsystem level. Assuming that the failure and success events of all SAS subsystem components are continuous exponentially distributed [116], where it is routinely used in the reliability analysis of realistic substations to determine the probability of failure/success for each SAS component over a time period of interest. We assume the study is undertaken for 60 months, i.e., t = 43,200 hours. Table 7.4 illustrates the failure rates of the SAS subsystems components and their probability values based on exponential distribution of each operational state [116], i.e. C_2 = 1 - $\text{e}^{(-\lambda_C t)}$ and $C_1 = \text{e}^{(-\lambda_C t)}$. The probabilities of the different SAS safety classes, which are calculated using $\mathbb{FETMA}$ are presented in Table 7.4.

To order to validate the results of the $\mathbb{FETMA}$ computations, we compare the SAS analysis results with those obtained through existing available techniques, as shown in Table 7.5: (1) manual FBD mathematical analysis using a paper and calculator, then calculating the failure/success probabilities of each consequence scenario; (2) commercial Isograph software for ET analysis; and (3) MCS using MATLAB based on random-based algorithm. It can be noticed from Table 7.5 that the results of safety classes for the SAS obtained from the $\mathbb{FETMA}$ analysis matches those

Table 7.4: Smart Automated Substation Probability of Components States

Comp.	λ *(f/yr)*	C_2	C_1	Comp.	λ *(f/yr)*	C_2	C_1
ACR	0.090	36.24%	63.76%	BCU	0.050	22.12%	77.88%
CB_1	0.085	34.62%	65.38%	PMU	0.040	18.13%	81.87%
CB_2	0.071	29.88%	70.12%	MC	0.055	24.04%	75.96%
CT_1	0.041	18.54%	81.46%	BPU	0.045	20.15%	79.85%
CT_2	0.057	24.79%	75.21%	ESW_1	0.087	35.27%	64.73 %
CT_3	0.046	20.55%	79.45%	ESW_2	0.094	37.49%	62.51%
CT_4	0.052	22.89%	77.11%	ESW_3	0.080	32.97%	67.03%
PT_1	0.045	20.15%	79.85%	ESW_4	0.095	37.81%	62.19%
PT_2	0.061	26.29%	73.71%	EI	0.083	33.97%	66.03%
PT_3	0.050	22.12%	77.88%	IPC	0.069	29.18%	70.82%
PT_4	0.063	27.02%	72.98%	HMI	0.100	39.35%	60.65%
MU_1	0.085	34.62%	65.38%	$Server_H$	0.020	9.52%	90.48%
MU_2	0.090	36.23%	63.77%	GW	0.073	30.58%	69.42%
MU_3	0.075	31.27%	68.73%	NCC	0.069	29.18%	70.82%
MU_4	0.080	32.97%	67.03%	PS	0.029	13.49%	86.51%

Table 7.5: Comparison for Smart Automated Substation Safety Classes Results

SAS Safety Classes	Manual	Isograph	MATLAB	$\mathbb{FETMA}$
SUCCESS	96.25%	96.251%	94.8743%	96.25117%
CLASS$_I$	1.54%	1.544%	2.3952%	1.54427%
CLASS$_{II}$	2.21%	2.205%	2.7305%	2.20456%
CPU Time	–	23.41 min	52.38 min	5.14 min

calculated using the analytical approach and Isograph, while MATLAB MCS provides slightly different results. Moreover, the CPU time for the SAS FBD analysis at the subsystem-level in $\mathbb{FETMA}$ is much faster than MATLAB MCS (10X) and Isograph (4X), as shown in Table 7.5. The taken time to build the model of the smart automated substation using the Isograph software and the MATLAB MCS were almost the same (a few hours each) but the $\mathbb{FETMA}$ analysis required less time for the modeling than both while the manual analysis required several days of modeling work.

Also, determining all possible safety classes at each automated substation subsystem level (Process Level, Bay Level, Station Level) almost in 5 minutes using the FETMA software saves the time-consuming as well as prevent cumbersome efforts to compute results using manual paper-and-pencil mathematical analysis by designers.

7.5.3 Sensitivity Analysis in FETMA

During the SAS safety analysis, difficult decisions for critical subsystem components redundancy need to be taken as this increases the total capital cost of the substation. For that purpose, sensitivity analysis is undertaken to determine the effect of adding backups on the safety of the entire SAS system. For instance, Figure 7.15 illustrates a redundant cascading topology [119] for the bay-level of the SAS system, which has an advantage of higher reliability compare to simple cascading while has a disadvantage of an extra cost for the SAS communication network. Moreover, in the SAS process-level, we assumed a redundant backup for the critical component ACR to improve the SAS performance. Figure 7.16 shows a comparison between the probabilistic risk assessment for all safety classes before and after redundancy using

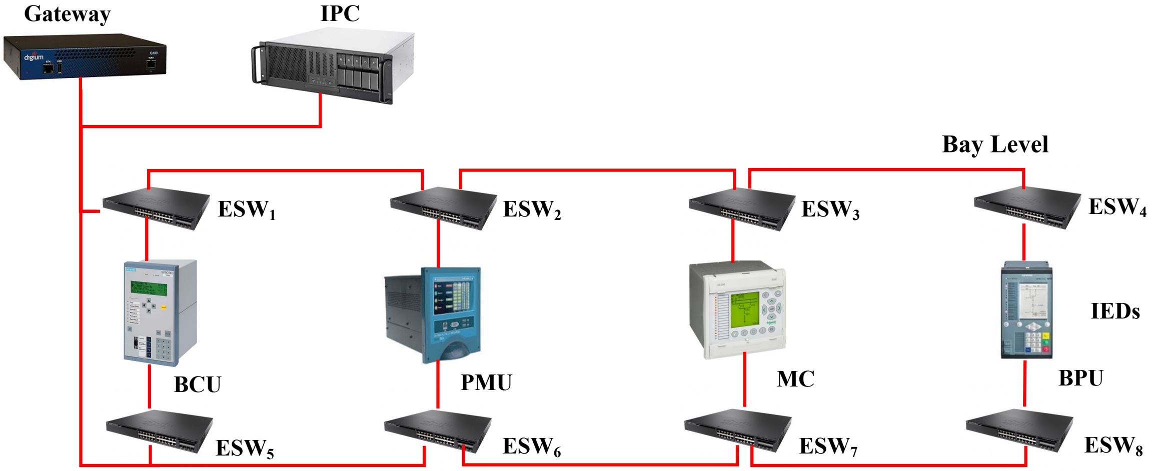


Figure 7.15: Smart Automated Substation Redundant Cascading Topology

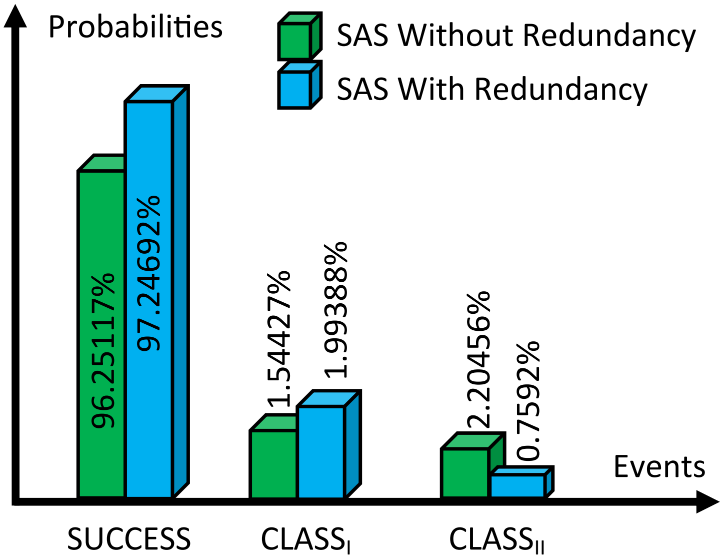


Figure 7.16: 𝔽𝔼𝕋𝕄𝔸: Automated Substation Classes Probabilistic Evaluation

the 𝔽𝔼𝕋𝕄𝔸 software in a histogram plot. It can be observed that the probability percentage of the SAS complete failure (CLASS$_{II}$) decreases from 2.20456% to 0.7592% by an amount of 1.44536%. Similarly, the proportions of the SAS success (SUCCESS) and manageable failure (CLASS$_I$) increases from 96.25117% to 97.24692% and from 1.54427% to 1.99388%, respectively. Using our novel 𝔽𝔼𝕋𝕄𝔸 software, we obtained the new results very easily by just adding the new elements and obtain the new results in around 5 minutes while it took around another 1 hour to get the results from MATLAB based on MCS as well as it was very cumbersome to repeat the whole FBD safety analysis for the complex SAS system manually. Therefore, we believe that 𝔽𝔼𝕋𝕄𝔸 may be liked by industrial power engineers to perform reliability and safety analysis of complex power systems for decision making at the design stage to obtain accurate and fast results. Performing the reliability analysis using our software 𝔽𝔼𝕋𝕄𝔸 on a realistic automated substation in a smart power grid, we clearly elucidate that our proposed 𝔽𝔼𝕋𝕄𝔸 provides the *first mechanical computation* software of FBD probabilities ever for subsystem-level safety analysis of complex systems.

7.6 Summary

In this chapter, we described a new software named $\mathbb{FETMA}$, which provides two features for event tree based reliability analysis of safety-critical systems at system and subsystem levels based on our ET/FBD formal modeling function of the concepts proposed by Papazoglou in [8] and [13], as well as the verified mathematical probabilistic formulations of ETs and FBDs in HOL4 described in Chapters 3 and 6 of this thesis. The $\mathbb{FETMA}$ software provides easy pop-up input windows for the ET and FBD modeling, reduction, partitioning and probabilistic evaluation functions, in order to facilitate users interactions. $\mathbb{FETMA}$ is implemented in Python and can be downloaded for use from [120]. The $\mathbb{FETMA}$ software saves time-consuming as well as cumbersome efforts for manual mathematical analysis for the probabilistic risk assessment of complex systems. Also, $\mathbb{FETMA}$ provides results of probabilistic risk assessment with much less CPU time compared to existing ET tools and random-based MCS algorithms. We have applied the two options of $\mathbb{FETMA}$ on a power transmission distance protection scheme and an automated substation system in a smart power grid.

Chapter 8

Conclusions and Future Work

Conclusions

Probabilistic risk assessment of safety-critical systems, such as smart power grids, has become more important to designers/planners at the critical design stage in order to ensure adequate and acceptable continuity of service without failures. In order to make decision-making of the optimal design for a safety-critical system, engineers require reliability evaluation of all possible consequences that can occur. Existing reliability analysis methods compromise the accuracy of the reliability parameters evaluation, which could lead to the occurrence of sudden accidents. Moreover, state-of-the-art techniques cannot handle n-level ETs, n-subsystems CCDs and multi-state FBDs.

Towards addressing these challenges, in this doctoral thesis, we proposed a novel methodology based on formal methods to conduct the system/subsystem-level reliability analysis of safety-critical systems as an accurate analysis approach. For that purpose, we formalized in HOL4 the notions of Event Trees (ET), Cause-Consequence Diagrams (CCD), Functional Block Diagrams (FBD) and verified mathematical formulations that can perform probabilistic evaluation of complex systems and based on any given probabilistic distribution, like Exponential/Weibull/Poisson. These verified probabilistic results can be used to compute accurate reliability indices, such as System/Customer Average Interruption Frequency/Duration Index (SAIFI, SAIDI and CAIDI), Average Service Availability/Unavailability Index (ASAI and ASUI).

The first contribution of this thesis is the formalization of ET constructs and analysis in HOL4, i.e., ET generation, ET reduction, ET partitioning and ET probabilistic evaluation. We verified probabilistic formulations that can be used in the probabilistic risk assessment of all possible risk scenarios of large-scale ET models that consist of $\mathcal{N}$ components and each component consists of $\mathcal{M}$-states. Subsequently, we performed the formal ET analyses of different levels of ET models for smart power grid applications, i.e., IEEE 3-bus bulk power grid; Québec-New England HVDC coupling between Canada and US; and IEEE 118-bus power network.

The second contribution is the formalization of FT/ET-based CCD structures, operations and probabilistic analysis in the HOL4 theorem prover. We verified probabilistic formulations, which enable planners/designers to perform formal probabilistic risk assessment of connected n-subsystems at each subsystem component level. As an application, we performed the formal FT/ET-based cause consequence analysis of the standard IEEE 39-bus distributed generation network system incorporating 50% Renewable Energy resources (RES) at each generation subsystem level.

The third contribution is the development of a novel idea of using RBDs instead of FTs in cause consequence analysis of safety-critical systems. We proposed new probabilistic formulations for multi-level CCDs based on RBDs and conducted their formalizations in HOL4, hence enabling formal RBD-based CCD analysis at the subsystem level. We applied this RBD/ET-based CCD formalization on a realistic smart power grid system consisting of four interconnected Micro-Grids incorporating 100% carbon-neutral power generation.

The next contributions of this thesis is the formalization of FBDs in HOL4. We formalized the FBD basic constructor FB, which can be used to build the mathematical expression of multi-levels FBDs based on multi-state subsystem components. We verified probabilistic theorems for all configurations of connected FBs for formal FBD analysis at the subsystem level. As an application, we conducted the formal subsystem-level FBD reliability analysis of a nuclear power plant and verified all possible safety classes of failure and reliability consequence events that can occur.

Finally, we developed a *Functional Block Diagram and Event Tree Modeling and Analysis* ($\mathbb{FETMA}$) software, which provides user-friendly interfaces and computes ET and FBD reliability analysis options for system and subsystem levels. We applied $\mathbb{FETMA}$ on a power transmission distance protection scheme and a smart automated substation in a smart power grid.

The results of all experimental outcomes have been compared to the state-of-the-art ET based reliability analysis approaches and tools and proved the superiority of the methods proposed in this thesis in terms of scalability, accuracy and CPU time. Some of the potential future enhancements and directions for further research are detailed in the next section.

Future Work

This thesis lays the ground for a promising framework for the formal ET based reliability analysis of safety-critical systems at the system and subsystem levels. Building on the proposed methodology and experimental results presented in this thesis, several enhancements and directions for further research can be explored and pursued.

- In its present form, the methodology considers only static consequence risk failure/reliability events at a specific instant of time t for which the reliability analysis is undertaken. An exciting extension of this work can be the integration of *dynamic* failure/reliability events, which preserve the history of sudden events occurrence in the required analysis. This would be a challenging research as it requires the formalization of mathematical formulas incorporated with continuous integration for N multi-states of failure and reliability of M multi-level components for Z connected subsystems all simultaneously together.

- The proposed formalization of subsystem-level cause consequence analysis considers is only either for *multi-level* failure or reliability assessment of connected n-subsystems (i.e., CCDs based on FTs or RBDs). An interesting extension of this work can be the formalization of both failure and reliability analysis CCD diagrams (i.e., CCDs based both FTs and RBDs), which will allow designers/-planners to provide the most suitable modeling to all connected subsystems of a safety-critical system. The formalization of such formulas is a bit challenging as it combines three formalizations FTs, RBDs and ETs simultaneously.

- The current version of the $\mathbb{FETMA}$ software is constructed in Python for the probabilistic risk assessment based on ET analysis and FBD analysis. An exciting extension of this framework can be the addition of cause consequence analysis based on FTs or RBDs or both combined together.

- The proposed reduction process of the multi-state ET analysis in HOL4 was done manually. It would be more efficient to automate the reduction process using SML functions. For instance, we could use a transformation process of ETs to Binary Decision Diagrams (BBD) for the special case of ETs with two-state models only (true and false) [17], and hence enable the use of some automatic BDD reduction algorithms.

- Using our proposed formal techniques for probabilistic risk assessment at system and subsystem levels, we can help electrical power utilities building the risk response plan (Step 3 of risk analysis) for recovery and restoration of modern power grids because of cyber threats at the critical design stage. This can be done by forecasting all risk consequences that can occur at different grid levels and prepare a complete backup plan in case of sudden unexpected accident events occurrence that could lead to a blackout of the whole grid.

- Finally, it would be interesting to integrate the rigorous analysis method for formal system/subsystem-level probabilistic evaluation of safety-critical systems in HOL4 and the user-friendly graphical interfaces of $\mathbb{FETMA}$ software. This could be done by constructing a *Python-HOL4 Parser* that provides the translation from $\mathbb{FETMA}$ to the HOL4 theorem prover and verse versa.

Bibliography

[1] T. Bedford, R. Cooke *et al.*, *Probabilistic Risk Analysis: Foundations and Methods.* Cambridge University Press, 2001.

[2] M. Yazdi, P. Hafezi, and R. Abbassi, "A Methodology for Enhancing the Reliability of Expert System Applications in Probabilistic Risk Assessment," *Journal of Loss Prevention in the Process Industries*, vol. 58, pp. 51–59, 2019.

[3] H. Kumamoto, *Satisfying Safety Goals by Probabilistic Risk Assessment.* Springer Science & Business Media, 2007.

[4] A. Hixenbaugh, "Fault Tree for Safety," Seattle, WA: The Boeing Company. D6-53604, Tech. Rep., 1968.

[5] J. Staley and P. Sutcliffe, "Reliability Block Diagram Analysis," *Microelectronics Reliability*, vol. 13, no. 1, pp. 33–47, 1974.

[6] K. Chung, "Markov Chains," *Springer-Verlag*, 1967.

[7] US Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants.* WASH-1400, NUREG-75/014, 1975, vol. 2.

[8] I. Papazoglou, "Functional Block Diagrams and Automated Construction of

Event Trees," *Reliability Engineering & System Safety*, vol. 61, no. 3, pp. 185–214, 1998.

[9] L. Ridley, "Dependency Modelling Using Fault-Tree and Cause-Consequence Analysis," Ph.D. dissertation, Loughborough University, UK, 2000.

[10] P. Gardoni, "Risk and Reliability Analysis," in *Risk and Reliability Analysis: Theory and Applications.* Springer, 2017, pp. 3–24.

[11] O. Hasan and S. Tahar, "Formal Verification Methods," in *Encyclopedia of Information Science and Technology.* IGI Global, 2015, pp. 7162–7170.

[12] R. Kennedy, C. Cornell, R. Campbell, S. Kaplan, and H. Perla, "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant," *Nuclear Engineering and Design*, vol. 59, no. 2, pp. 315–338, 1980.

[13] I. Papazoglou, "Mathematical Foundations of Event Trees," *Reliability Engineering & System Safety*, vol. 61, no. 3, pp. 169–183, 1998.

[14] Q. Chen, "The probability, Identification, and Prevention of Rare Events in Power Systems," Ph.D. dissertation, Iowa State University, US, 2004.

[15] D. Peplow, C. Sulfredge, R. Sanders, R. Morris, and T. Hann, "Calculating Nuclear Power Plant Vulnerability Using Integrated Geometry and Event/Fault-Tree Models," *Nuclear Science and Engineering*, vol. 146, no. 1, pp. 71–87, 2004.

[16] Y. Phulpin, J. Hazra, and D. Ernst, "Model Predictive Control of HVDC Power Flow to Improve Transient Stability in Power Systems," in *International Conference on Smart Grid Communications.* IEEE, 2011, pp. 593–598.

[17] V. Muzik and Z. Vostracky, "Possibilities of Event Tree Analysis Method for Emergency States in Power Grid," in *International Scientific Conference on Electric Power Engineering.* IEEE, 2018, pp. 1–5.

[18] Isograph Software, 2021. [Online]. Available: https://www.isograph.com

[19] SoHAR Software, 2021. [Online]. Available: http://www.sohar.com/reliability-software/eta.html

[20] ReliaSoft Software, 2021. [Online]. Available: https://www.reliasoft.com

[21] ITEM Software, 2021. [Online]. Available: https://itemsoft.com/eventtree.html

[22] N. Thomopoulos, *Essentials of Monte Carlo Simulation: Statistical Methods for Building Simulation Models.* Springer Science & Business Media, 2012.

[23] G. Vanorio and J. Mera, "Methodology for Risk Analysis in Railway Tunnels using Monte Carlo Simulation," *WIT Transactions on the Built Environment*, vol. 127, pp. 673–683, 2012.

[24] X. Yu and C. Singh, "A Practical Approach for Integrated Power System Vulnerability Analysis with Protection Failures," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1811–1820, 2004.

[25] G. Sugumar, R. Selvamuthukumaran, M. Novak, and T. Dragicevic, "Supervisory Energy-Management Systems for Microgrids: Modeling and Formal Verification," *IEEE Industrial Electronics Magazine*, vol. 13, no. 1, pp. 26–37, 2019.

[26] N. Papakonstantinou, S. Sierla, B. O'Halloran, and Y. Tumer, "A Simulation based Approach to Automate Event Tree Generation for Early Complex System Designs," in *Design Engineering Technical Conferences and Computers and*

Information in Engineering Conference, vol. 55867. American Society of Mechanical Engineers, 2013, pp. 1–10.

[27] J. Andrews and L. Ridley, "Application of the Cause-Consequence Diagram Method to Static Systems," *Reliability Engineering & System Safety*, vol. 75, no. 1, pp. 47–58, 2002.

[28] J. Andrews, "Reliability of Sequential Systems Using the Cause—Consequence Diagram Method," *Journal of Process Mechanical Engineering*, vol. 215, no. 3, pp. 207–220, 2001.

[29] G. Vyzaite, S. Dunnett, and J. Andrews, "Cause-Consequence Analysis of Non-Repairable Phased Missions," *Reliability Engineering & System Safety*, vol. 91, no. 4, pp. 398–406, 2006.

[30] O. Nỳvlt and M. Rausand, "Dependencies in Event Trees Analyzed by Petri Nets," *Reliability Engineering & System Safety*, vol. 104, pp. 45–57, 2012.

[31] F. Ortmeier, W. Reif, and G. Schellhorn, "Deductive Cause-Consequence Analysis," *IFAC Proceedings Volumes*, vol. 38, no. 1, pp. 62–67, 2005.

[32] SMV Moder Checker, 2021. [Online]. Available: http://www.cs.cmu.edu/~modelcheck/smv.html

[33] International Electrotechnical Commission, IEC 61850, 2021. [Online]. Available: https://webstore.iec.ch/publication/6028

[34] European Committee for Electrotechnical Standardization, EN 50128, 2020. [Online]. Available: https://www.cenelec.eu/dyn/www/f?p=104:110:473366572216601::::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:1258773,68080,25

[35] International Standardization Organization, ISO 26262, 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en

[36] M. Nawaz, M. Malik, Y. Li, M. Sun, and M. Lali, "A Survey on Theorem Provers in Formal Methods," 2019. [Online]. Available: arXivpreprintarXiv:1912.03028

[37] HOL4 Theorem Prover, 2021. [Online]. Available: https://hol-theorem-prover.org

[38] Isabelle Theorem Prover, 2021. [Online]. Available: https://isabelle.in.tum.de/

[39] PVS Theorem Prover, 2021. [Online]. Available: https://pvs.csl.sri.com/

[40] J. Harrison, "HOL light: An Overview," in *International Conference on Theorem Proving in Higher Order Logics*. Springer, 2009, pp. 60–66.

[41] Coq Theorem Prover, 2021. [Online]. Available: https://coq.inria.fr/

[42] W. Ahmad, "Formal Dependability Analysis using Higher-Order-Logic Theorem Proving," Ph.D. dissertation, National University of Sciences and Technology, Islamabad, Pakistan, 2017.

[43] Y. Elderhalli, "Dynamic Dependability Analysis using HOL Theorem Proving with Application in Multiprocessor Systems," Ph.D. dissertation, Concordia University Montréal, Québec, Canada, 2019.

[44] A. Mahmood, O. Hasan, H. Gillani, Y. Saleem, and S. Hasan, "Formal Reliability Analysis of Protective Systems in Smart Grids," in *Region 10 Symposium*. IEEE, 2016, pp. 198–202.

[45] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid—The New and Improved Power Grid: A Survey," *IEEE Communication Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[46] A. Khurram, H. Ali, A. Tariq, and O. Hasan, "Formal Reliability Analysis of Protective Relays in Power Distribution Systems," in *Formal Methods for Industrial Critical Systems.* Springer, 2013, pp. 169–183.

[47] G. Sugumar, R. Selvamuthukumaran *et al.*, "Formal Validation of Supervisory Energy Management Systems for Microgrids," in *Industrial Electronics Society.* IEEE, 2017, pp. 1154–1159.

[48] K. Larsen, P. Pettersson, and W. Yi, "UPPAAL in a Nutshell," *Software Tools for Technology Transfer*, vol. 1, no. 1-2, pp. 134–152, 1997.

[49] T. Badings, A. Hartmanns, N. Jansen, and M. Suilen, "Balancing Wind and Batteries: Towards Predictive Verification of Smart Grids," in *NASA Formal Methods Symposium*, ser. LNCS, vol. 12673. Springer, 2021, pp. 1–18.

[50] Y. Li, P. Zhang, and P. Luh, "Formal Analysis of Networked Microgrids Dynamics," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3418–3427, 2017.

[51] CORA Manual, 2015. [Online]. Available: http://archive.www6.in.tum.de/www6/pub/Main/SoftwareCORA/Cora2015Manual.pdf

[52] W. Ahmad, O. Hasan, F. Awwad, N. Bastaki, and S. Hasan, "Formal Reliability Analysis of an Integrated Power Generation System Using Theorem Proving," *IEEE Systems Journal*, vol. 14, no. 4, pp. 4820–4831, 2020.

[53] W. Ahmad, O. Hasan, and S. Tahar, "Formal Reliability and Failure Analysis of Ethernet based Communication Networks in a Smart Grid Substation," *Formal Aspects of Computing*, vol. 32, no. 1, pp. 71–111, 2020.

[54] G. VanRossum and F. Drake, *The Python Language Reference.* Python Software Foundation Amsterdam, 2010.

[55] K. Lee, "Language Implementation in Standard ML," in *Programming Languages.* Springer, 2008, pp. 1–34.

[56] J. Grainger and W. Stevenson, *Power System Analysis.* McGraw-Hill, 2003.

[57] A. Keyhani and M. Albaijat, *Smart Power Grids.* Springer Science & Business Media, 2012.

[58] B. Xin, L. Wan, J. Yu, and W. Dang, "Basic Event Probability Determination and Risk Assessment Based on Cause-Consequence Analysis Method," in *Journal of Physics*, vol. 1549, no. 5. IOP Publishing, 2020, p. 052094.

[59] A. Pérez, C. Borges, and J. Rodríguez, "Photovoltaic System Proposal for a House," *International Journal of Physical Sciences and Engineering*, vol. 3, no. 2, pp. 34–43, 2019.

[60] A. Alferidi and R. Karki, "Development of Probabilistic Reliability Models of Photo-Voltaic system Topologies for System Adequacy Evaluation," *Applied Sciences*, vol. 7, no. 2, p. 176, 2017.

[61] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, and R. Akbarpour, "Formal Reasoning About Expectation Properties for Continuous Random Variables," in *Formal Methods*, ser. LNCS 5850. Springer, 2009, pp. 435–450.

[62] M. Čepin, *Assessment of Power System Reliability: Methods and Applications.* Springer Science & Business Media, 2011.

[63] N. Limnios, *Fault Trees.* John Wiley & Sons, 2013.

[64] K. Trivedi and A. Bobbio, "Reliability Block Diagrams," in *Reliability and Availability Engineering: Modeling, Analysis, and Applications.* Cambridge University Press, 2017, pp. 105–149.

[65] Y. Hegazy and M. Mostafa, "Reliability Indices of Electrical Distributed Generation Systems," *IEEE Transactions on Power Systems*, vol. 4, no. 10, pp. 1785–1790, 2005.

[66] R. Billinton and R. Allan, *Reliability Assessment of Large Electric Power Systems.* Springer Science & Business Media, 2012.

[67] S. Kaur, A. Singh, and R. Khela, "Load Flow Analysis of IEEE 3-Bus System by using Mipower Software," *Journal of Engineering Research & Technology*, vol. 4, no. 03, pp. 9–16, 2015.

[68] The HOL System Reference, 2021. [Online]. Available: http://sourceforge.net/projects/hol/files/hol/kananaskis-14/kananaskis-14-reference.pdf/download

[69] G. Anders and A. Vaccaro, *Innovations in Power Systems Reliability.* Springer, 2011.

[70] W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods.* Springer Science & Business Media, 2013.

[71] M. Abdelghany, "ET Formalization in HOL4," 2021. [Online]. Available: https://github.com/hvg-concordia/ET

[72] A. Pradhan, S. Kar *et al.*, "Implementation of Monte Carlo Simulation to the Distribution Network for Its Reliability Assessment," in *Innovation in Electrical Power Engineering, Communication, and Computing Technology.* Springer, 2020, pp. 219–228.

[73] D. Dickmander, S. Lee, G. Desilets, and M. Granger, "AC/DC Harmonic Interactions in the Presence of GIC for the Quebec-New England Phase II HVDC Transmission," *IEEE Transactions on Power Delivery*, vol. 9, no. 1, pp. 68–78, 1994.

[74] D. Gan, R. Thomas, and R. Zimmerman, "Stability-Constrained Optimal Power Flow," *IEEE Transaction on Power Systems*, vol. 15, no. 2, pp. 535–540, 2000.

[75] G. Morin, L. Bui, S. Casoria, and J. Reeve, "Modeling of the Hydro-Quebec-New England HVDC system and Digital Controls with EMTP," *IEEE Transactions on Power Delivery*, vol. 8, no. 2, pp. 559–566, 1993.

[76] E. Dialynas, N. Koskolos, and D. Agoris, "Reliability Assessment of Autonomous Power Systems Incorporating HVDC Interconnection Links," *IEEE Transactions on Power Delivery*, vol. 11, no. 1, pp. 519–525, 1996.

[77] F. Marvasti and A. Mirzaei, "Hybrid Travelling Wave/Distance Protection for HVDC Transmission Lines based on Phase Angles of Characteristic Harmonic Impedances," *Electrical Engineering*, pp. 1–14, 2021.

[78] I. Pena, B. Martinez-Anido, and B. Hodge, "An Extended IEEE 118-Bus Test System with High Renewable Penetration," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 281–289, 2017.

[79] V. Yadav and P. Ghoshal, “Optimal Power Flow for IEEE 30 and 118-Bus Systems Using Monarch Butterfly Optimization,” in *Technologies for Smart-City Energy Security and Power*. IEEE, 2018, pp. 1–6.

[80] M. Marzband, M. Moghaddam *et al.*, “Adaptive Load Shedding Scheme for Frequency Stability Enhancement in Microgrids,” *Electric Power Systems Research*, vol. 140, pp. 78–86, 2016.

[81] G. Bhatt and S. Affljulla, “Analysis of Large Scale PV Penetration Impact on IEEE 39-Bus Power System,” in *Riga Technical University Conference on Power and Electrical Engineering*. IEEE, 2017, pp. 1–6.

[82] H. Gils and S. Simon, “Carbon Neutral Archipelago-100% Renewable Energy Supply for the Canary Islands,” *Applied Energy*, vol. 188, pp. 342–355, 2017.

[83] D. Sarkar, *Thermal Power Plant: Design and Operation*. Elsevier, 2015.

[84] M. Abdelghany, “FT/ET based Cause-Consequence Formalization in HOL4,” 2021. [Online]. Available: https://github.com/hvg-concordia/CCD

[85] Y. Papadopoulos, M. Walker, D. Parker, E. Rüde, R. Hamann, A. Uhlig, U. Grätz, and R. Lien, “Engineering Failure Analysis and Design Optimisation with HiP-HOPS,” *Engineering Failure Analysis*, vol. 18, no. 2, pp. 590–608, 2011.

[86] H. Jahanian, D. Parker, M. Zeller, A. McIver, and Y. Papadopoulos, “Failure Mode Reasoning in Model Based Safety Analysis,” 2020. [Online]. Available: https://arxiv.org/abs/2005.06279

[87] H. Jahanian, “Failure Mode Reasoning,” in *International Conference on System Reliability and Safety*. IEEE, 2019, pp. 295–303.

[88] S. Kabir, K. Aslansefat, I. Sorokos, Y. Papadopoulos, and Y. Gheraibia, "A Conceptual Framework to Incorporate Complex Basic Events in HiP-HOPS," in *Model-Based Safety and Assessment*, ser. LNCS, vol. 11842. Springer, 2019, pp. 109–124.

[89] F. Porté-Agel, M. Bastankhah, and S. Shamsoddin, "Wind-Turbine and Wind-Farm Flows: a Review," *Boundary-Layer Meteorology*, vol. 174, no. 1, pp. 1–59, 2020.

[90] S. Jaiswal and G. Pahuja, "Effect of Reliability of Power Converters in Productivity of Wind Turbine," in *Conference on Power Electronics.* IEEE, 2014, pp. 1–6.

[91] S. Muller, M. Deicke, and R. De Doncker, "Doubly Fed Induction Generator Systems for Wind Turbines," *Industry Applications Magazine*, vol. 8, no. 3, pp. 26–33, 2002.

[92] W. Shepherd and L. Zhang, *Power Converter Circuits.* CRC Press, 2004.

[93] M. Abdelghany, "RBD/ET based Cause-Consequence Formalization in HOL4," 2021. [Online]. Available: https://github.com/hvg-concordia/CCD_RBD

[94] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *Power and Energy Magazine*, vol. 5, no. 4, pp. 78–94, 2007.

[95] O. Palizban and K. Kauhaniemi, "Microgrid Control Principles in Island Mode Operation," in *Grenoble Conference.* IEEE, 2013, pp. 1–6.

[96] O. Egbue, D. Naidu, and P. Peterson, "The Role of Microgrids in Enhancing Macrogrid Resilience," in *Smart Grid and Clean Energy Technologies.* IEEE, 2016, pp. 125–129.

[97] P. Sampaio and M. González, "Photovoltaic Solar Energy: Conceptual Framework," *Renewable and Sustainable Energy Reviews*, vol. 74, pp. 590–601, 2017.

[98] R. Yokoyama, T. Niimura, and N. Saito, "Modeling and Evaluation of Supply Reliability of Microgrids including PV and Wind Power," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century.* IEEE, 2008, pp. 1–5.

[99] Z. Li, Y. Yuan, and F. Li, "Evaluating the Reliability of Islanded Microgrid in an Emergency Mode," in *Universities Power Engineering Conference.* IEEE, 2010, pp. 1–5.

[100] T. Adefarati, R. Bansal, and J. Justo, "Reliability and Economic Evaluation of a Microgrid Power System," *Energy Procedia*, vol. 142, pp. 43–48, 2017.

[101] R. Karki and R. Billinton, *Reliability Modeling and Analysis of Smart Power Systems.* Springer Science & Business Media, 2014.

[102] R. Ross, *Reliability Analysis for Asset Management of Electric Power Grids.* Wiley Online Library, 2019.

[103] R. Moharil and P. Kulkarni, "Reliability Analysis of Solar PhotoVoltaic System using Hourly Mean Solar Radiation Data," *Solar Energy*, vol. 84, no. 4, pp. 691–702, 2010.

[104] P. J. Tavner, J. Xiang, and F. Spinato, "Reliability Analysis for Wind Turbines," *Journal for Progress and Applications in Wind Power Conversion Technology*, vol. 10, no. 1, pp. 1–18, 2007.

[105] J. Lee and N. McCormick, *Risk and Safety Analysis of Nuclear Systems.* John Wiley & Sons, 2011.

[106] J. Choi and H. Seok, "Development of Risk Assessment Framework and the Case Study for a Spent Fuel Pool of a Nuclear Power Plant," *Nuclear Engineering and Technology*, 2020.

[107] M. Abdelghany, "Functional Block Diagrams Formalization in HOL4," 2020. [Online]. Available: https://github.com/hvg-concordia/FBD

[108] "PyGraphviz Python package," 2021. [Online]. Available: https://pygraphviz.github.io/

[109] L. Hewitson, M. Brown, and R. Balakrishnan, *Practical Power System Protection.* Elsevier, 2004.

[110] E. Portante, S. Folga, J. Kavicky, and L. Malone, "Simulation of the September 8, 2011, San Diego Blackout," in *Winter Simulation Conference*, Savannah, US, 2014, pp. 1527–1538.

[111] M. Eissa, "Ground Distance Relay Compensation based on Fault Resistance Calculation," *IEEE Transactions on Power Delivery*, vol. 21, no. 4, pp. 1830–1835, 2006.

[112] S. Xu, Y. Qian, and R. Q. Hu, "On Reliability of Smart Grid Neighborhood Area Networks," *IEEE Access*, vol. 3, pp. 2352–2365, 2015.

[113] M. Aftab, S. Hussain, I. Ali, and T. Ustun, "IEC 61850 Based Substation Automation System: A Survey," *Journal of Electrical Power & Energy Systems*, vol. 120, p. 106008, 2020.

[114] J. König and L. Nordström, "Reliability Analysis of Substation Automation System Functions," in *Reliability and Maintainability Symposium.* IEEE, 2012, pp. 1–6.

[115] S. R. Palakodeti, H. Guo, and P. Raju, “Reliability Modeling and Simulation of Electric Substations–A Case Study,” *Applications of Modelling and Simulation*, vol. 5, pp. 35–43, 2021.

[116] H. Hajian-Hoseinabadi and H. Golshan, “Availability, Reliability, and Component Importance Evaluation of Various Repairable Substation Automation Systems,” *IEEE Transactions on Power Delivery*, vol. 27, no. 3, pp. 1358–1367, 2012.

[117] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, “Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2442–2451, 2017.

[118] F. Wang, W. Tuinema, M. Gibescu, and A. van der Meijden, “Reliability Evaluation of Substations Subject to Protection System Failures,” in *Grenoble Conference*. IEEE, 2013, pp. 1–6.

[119] F. Salehi, A. Brahman, R. Keypour, and W. Lee, “Reliability Assessment of Automated Substation and Functional Integration,” in *Industry Applications Society Annual Meeting*. IEEE, 2016, pp. 1–7.

[120] M. Abdelghany, “FETMA Software,” 2021. [Online]. Available: https://github.com/hvg-concordia/FETMA

Biography

Education

- **Concordia University**: Montreal, Quebec, Canada.

  Ph.D., Electrical & Computer Engineering (January 2018 - September 2021)

  Thesis Title : Formal Probabilistic Risk Assessment using Theorem Proving with Applications in Power Systems

- **Ain-Shams University**: Cairo, Egypt.

  M.Sc, Power Engineering (April 2014 - December 2016)

  Thesis Title : Optimal Demand Energy Management for Smart Distribution Networks

- **Ain-Shams University**: Cairo, Egypt.

  B.Sc, Power Engineering (September 2008 - June 2012)

  Cumulative Grade : Excellent with Honor (91.03%)

  Cumulative Rank : 1^{st} in Class (out of 294 students)

Awards

- Concordia University Doctoral Accelerator Award, March 2021 (5,000 C$).
- Concordia International Tuition Award of Excellence, January 2018 - December 2020 (35,949 C$).
- Concordia Conference and Exposition Award, October 2020 (363 C$).
- Concordia Conference and Exposition Award, December 2019 (980 C$).

Work History

- **Research Assistant**, Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada (January 2018 - September 2021).
- **Part-Time Teaching Assistant**, Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada (January 2019 - May 2021).
- **Assistant Lecture**, Department of Electrical Power and Machines, Ain-Shams University, Cairo, Egypt (September 2012 - December 2017).
- **Part-Time Projects Control Team Leader**, ProService, Engineering Company for Electrical Power Projects, Cairo, Egypt (March 2014 - December 2017).
- **Part-Time Electrical Power Site Supervisor**, Consulting Engineering Center, Ain-Shams University, Cairo, Egypt (August 2014 - December 2017).

Publications

- ## Journal Papers

  - **Bio-Jr1** M. Abdelghany and S. Tahar, ”Multi-State Reliability Evaluation of Québec-New England HVDC using Formal Methods,” IEEE Transactions on Power Delivery, July 2021. *Submitted*

  - **Bio-Jr2** M. Abdelghany, S. Tahar, and S. Nethula, ”𝔽𝔼𝕋𝕄𝔸: A Software for Functional Block Diagram and Event Tree based Safety Analysis,” IEEE Transactions on Industrial Informatics, July 2021. *Submitted*

  - **Bio-Jr3** M. Abdelghany and S. Tahar, ”Predictive Verification of Reliability Evaluation for Multiple Interconnected Micro-Grids,” IEEE Transactions on Power Systems, June 2021. *Submitted.*

  - **Bio-Jr4** M. Abdelghany, W. Ahmad, and S. Tahar, ”Event Tree Reliability Analysis of Safety Critical Systems Using Theorem Proving,” IEEE Systems Journal, May 2021. Available: https://doi.org/10.1109/JSYST.2021.3077558

  - **Bio-Jr5** M. Abdelghany and S. Tahar, ”Cause-Consequence Diagram Reliability Analysis using Formal Techniques with Application to Electrical Power Networks,” IEEE Access, Vol. 9, pp. 23929-23943, January 2021.

- **Conference Papers**

  - **Bio-Cf1** M. Abdelghany and S. Tahar, ”Functional Block Diagram based Safety Analysis of Complex Systems using Theorem Proving,” 10th International Conference on Certified Programs and Proofs, September 2021. *Submitted*

  - **Bio-Cf2** M. Abdelghany and S. Tahar, ”Formalization of RBD-based Cause Consequence Analysis in HOL,” in 14th Conference on Intelligent Computer Mathematics, ser. LNCS, Vol 12833. Springer, July 2021, pp. 47-64, Timisoara, Romania.

  - **Bio-Cf3** M. Abdelghany, W. Ahmad, and S. Tahar, ”Event Tree Reliability Analysis of Electrical Power Generation Network using Formal Techniques,” in 20th Electric Power and Energy Conference, IEEE, November 2020, pp. 1-7, Edmonton, Canada.

  - **Bio-Cf4** M. Abdelghany, A. Magdy and W. El-Khattam, ”Optimal Demand Management for Smart Distribution Networks,” in 20th Electric Power and Energy Conference, IEEE, November 2020, pp. 1-7, Edmonton, Canada.

  - **Bio-Cf5** M. Abdelghany, W. Ahmad, S. Tahar, and S. Nethula, ”$\mathcal{ETMA}$: An Efficient Tool for Event Trees Modeling and Analysis, ” in 14th International Systems Conference, IEEE, August 2020, pp. 1-8, Montreal, Canada.

- **Bio-Cf6** M. Abdelghany, A. Magdy and W. El-Khattam, ”Optimal Load Scheduling for Smart Distribution Networks using Genetic Algorithm,” in 17^{th} Middle East Power Systems Conference, IEEE, December 2015, pp. 1-5, Mansoura, Egypt.

• Book Chapter

- **Bio-Ch1** M. Abdelghany, and S. Tahar, ”Reliability Analysis of Smart Grids using Formal Methods,” Handbook of Smart Energy Systems, June 2021. *Accepted*

• Technical Reports

- **Bio-Tr1** M. Abdelghany, and S. Tahar, ”Formal FT-based Cause-Consequence Reliability Analysis using Theorem Proving,” Technical Report, January 2021. Available: https://arxiv.org/abs/2101.07174

- **Bio-Tr2** M. Abdelghany, W. Ahmad, S. Tahar, and S. Nethula, ”ETMA: A New Software for Event Tree Analysis with Application to Power Protection,” Technical Report, June 2020. Available: https://arxiv.org/abs/2006.12383

- **Bio-Tr3** M. Abdelghany, W. Ahmad, and S. Tahar, ”A Formally Verified HOL4 Algebra for Event Trees,” Technical Report, April 2020. Available: http://arxiv.org/abs/2004.14384