energies

MDPI

Article

Risk Assessment of Micro Energy Grid Protection Layers

Hossam A. Gabbar [1,2,*] and Yahya Koraz [2]

[1] Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology, 2000 Simcoe Street North, Oshawa, ON L1H7K4, Canada

[2] Faculty of Engineering and Applied Science, University of Ontario Institute of Technology, 2000 Simcoe Street North, Oshawa, ON L1H7K4, Canada; Yahya.koraz@uoit.ca

* Correspondence: Hossam.Gabbar@uoit.ca; Tel.: +1-905-721-8668 (ext. 5497)

Academic Editor: Gianfranco Chicco
Received: 13 June 2017; Accepted: 3 August 2017; Published: 10 August 2017

Abstract: Micro energy grids (MEGs) are used extensively to meet the combined electricity, heating, and cooling energy demands for all types of customers. This paper develops a hazard matrix for a MEG and utilizes two advanced risk modeling approaches (fault tree and layer of protection analysis (*LOPA*)) for MEGs' risk analysis. A number of independent protection layers (IPLs) have been proposed to achieve a resilient MEG, hence increasing its safety integrity level (SIL). IPLs are applied using co-generators and thermal energy storage (TES) techniques to minimize the hazards of system failure, increase efficiency, and minimize greenhouse gas emissions. The proposed modeling and risk assessment approach aims to design a resilient MEG, which can utilize those potentials efficiently. In addition, an energy risk analysis has been applied on each MEGs' physical domains such as electrical, thermal, mechanical and chemical. The concurrent objectives achieve an increased resiliency, reduced emissions, and sustained economy.

Keywords: micro energy grid (MEG); risk assessment; layer of protection analysis (*LOPA*); fault tree analysis; independent protection layer (IPL)

1. Introduction

A micro energy grid (MEG) can be defined as a local distribution system that comprises energy sources, distribution lines, metering infrastructure, and computing/control systems. MEGs may integrate numerous types of renewable energy sources such as solar photovoltaic (PV), wind turbine (WT), small hydro, geothermal, waste-to-energy, and combined heat and power systems (CHPs) [1].

MEGs have promising contributions in achieving efficient utilization of renewable energy and in improving the resiliency of energy distribution grids. MEGs reduce energy losses and increase their self-healing capability by utilizing multi-local sources and adaptive grid topology [2]. MEGs provide accumulative/integrated multi-energy systems (i.e., electricity, cooling, and heating energy) [3]. MEGs include distributed generators, energy storage devices, predictive energy management to reduce both electricity costs and emissions, as well as improve energy reliability and efficiency [4]. From the system's perspective, a MEG as one controllable unit which combines local energy sources, and energy storage units, has the capability of being self-sufficient to cover electricity, cooling, and heating demands for its local customers.

A MEG can apply adaptive control/scheduling algorithms to its local energy sources to realize autonomous operations during normal and/or peak demands. Moreover, those adaptive algorithms facilitate self-healing capability during main/upstream grid failure. This is because a MEG can operate independently as an isolated unit by using its generation nodes and energy storage units to cover its local demands.

Effective design of a fault-tolerant management system of a MEG realizes the full capability of resiliency and eco-friendly energy production. A MEG is comprised of complex systems with varied response characteristics at various time-scales. Therefore, a hierarchical pattern is recommended for the control topology of such complex systems [5,6]. It includes an overall supervisory control independent protection layer (IPL), which determines the set-points of the significant operation parameters of the MEG based on energy demand. For instance, the decision of which distributed energy resources (DERs) should be operating (on/off states) and at what conditions they must be operating (energy levels, power levels, temperatures, pressures, mass flow rates, and so on) [7]. Several advantages can be gained by utilizing resilient MEGs, as listed below:

- Enhance the reliability of the system's performance,
- Enhance customers' awareness and choices,
- Encourage efficient decisions to be taken by the utility providers,
- Better match between energy generation and energy use, and hence lower cost and/or losses.

When resilient MEG technology is applied to a city, the city is called a "Smart Green City", such as Canada's Dockside or the UAE's Masdar. On the other hand, incorporating multi-DERs, particularly renewable energy sources (RES), into existing energy grids offers significant challenges due to the intermittent and varying characteristics of the environment, Further to the uncertainty of dealing with indefinite systems' behaviors, which means constructing large complex system, MEGs, is associated with high risk levels [8]. Thus, there is an increased demand for designs of MEGs with higher safety fault tolerances against numerous types of risks, compared with the various discrete systems that have been used earlier [9,10]. Hereby, the risk analysis becomes a fundamental part of practical MEG.

1.1. Hazard and Risk Analysis Literature Review

A layered fault tree model was modified in ref. [11] to differentiate between islanded and grid connected modes for the micro-grid (MG). The hierarchical Monte Carlo simulation method was utilized to examine the system's reliability, by combining power sufficiency assessment with system failure insights. The design concept was enhanced based on the assumption that the load priority measures are sufficient to define the weak part of the system.

In [12], a comparison study between Bahill and Haimes risk analysis approaches was justified, and a case study of the risk of incorporating solar photovoltaic systems into a commercial electric power grid was presented. The study shows the strengths and the weaknesses of each approach.

A new design for a process named Diogenes was revealed in [13]. Diogenes helps systems' engineers to identify the unintended, but predictable, consequences of fault propagation for new systems under design.

An efficient multiplayer collaboration framework was presented in ref. [14], to characterize sources of system risk from various expert opinions. It can be considered as a key solution for unstructured, multidimensional problems.

Reference [15], introduces risk analyses for pinewood derbies, and also shows several risk analysis techniques and presents the problems accompanying with them.

The article [16], proposes and implements a real-time distributed measuring nodes network to diagnose faults in uninterruptible high-power supply systems and high-power transformers of MG used for railway interlocking signaling installations. The proposed methodology is based on the thermal and electrical symptoms analysis and the mechanical degradation index by measuring the vibration.

A failure mode and effect analysis (FMEA) approach was presented in [17], for fault diagnosis of energy storage unit, Valve Regulated Lead-Acid batteries, and 3-phase high power transformers, utilized in switching converters and power isolation. The FMEA approach utilizes a distributed measuring nodes network, described in [16], based on electrical (voltage, current, impedance) and thermal degradation analysis and vibration-based mechanical stress diagnosis.

Many safety instrumented function (SIF) hardware was integrated into energy distribution grids to protect human, premises and equipment from the negative consequences of the failure propagation. Hereinafter some cutting edge technologies of SIF in are presented.

Reference [18] presents a fault detection, isolation, and service restoration (FDIR) for an outage event in an electrical distribution grids. An intelligent power switch with integrated protections and self-diagnostic was proposed in ref. [19], by using HV-CMOS technology to safely handle the ordinary and extraordinary automotive electrical and environmental conditions.

Zero sequence components were described in [20] for micro grid protection of single line to ground faults and [21] utilizes negative sequence components of the line current for protection of line to line faults. A survey on protection requirements of dc-micro grid was illustrated in [22,23]. Numerous types of intelligent relays were proposed for micro grids that consist of various types of energy sources [24,25]. Plug and play function was proposed in [26] by creating an IEC 61850 information structure of a micro energy grid. The proposal aims to create standards for design, operation and protection of micro grids.

1.2. Definition of Risk

Risk is an essential factor in any system's safety design, where, risk can be defined by the potential harm or loss correlated with an activity performed in an uncertain circumstance. The first use of "risk" was in 1667, by Arnauld and Nicole, who assumed it consisted of at least two components. "Fear of some harm ought to be proportional not only to the magnitude of the harm, but also to the probability of the event" [27].

There are different methods to identify and quantify risks. Below are illustrated discussions of the existing quantifying risk methods:

(1) Haimes, in [28], uses accumulate summation of the probability density function of the severity of consequences and a random variable of the severity of consequences; thus, the frequency of occurrence of the hazard is latent.

(2) Bahill, in [29], uses a different method for quantifying the risk by combining the function of frequency of occurrence with the severity of failure consequences. Bahill's method is commonly used in North American industries.

(3) In [30] two combining functions were illustrated:

   I- Linearly combining functions that accumulate the summation of the combined products of the weight of importance with the score variable. Weight of importance is a random variable between 0 and 1.

   II- Product combining functions that accumulate the products of the score variable to the power of the weight of importance.

(4) Exponential combining functions [31], that utilizes an exponent of the summation of a linear combining function between the weight of importance and score variable. Hence, a constant variable may used for calibration purpose.

(5) Sum minus product combining function [32], which derived from the probability of unions between independent variables. However, this function is lacking when used to qualify the risk, where if severity or likelihood is 0 then the risk should be 0, which is not the case by using this equation.

(6) Compromised combining function [33], that deploys two weight variables with two different score variables.

(7) Reference [34] presents risk by doubling the severity weight multiplied by the frequency of fault event occurrence.

(8) In [35] the failure modes and effects analysis (FEMA) comprises the difficulty of detection. It consists product of frequency of occurrence, severity of failure consequences and difficulty of detection.

(9) The hazard level can be also a product of the consequences severity and the fault class [36], fault class is a combination of the probability of failure, the fault event frequency and the system's ability to avoid failure occasion.

2. Problem Definition

Micro energy grid (MEG) was initiated to overcome the challenges on energy supply and distribution [37]. However, details about the safety design of MEGs are unavailable, which is essential for obtaining resilient MEG. Failure in any component such as DERs might increase the hazard(s) of demand not served (DNS) and/or blackouts/brownouts. Furthermore, utilization of on-site renewables sources (RES) have accompanying intermittency that may affect the integrity of MEGs. Thus, MEGs require a high adaptive performance from the distributed energy systems.

Faults in MEGs, if not controlled properly, might propagate and cause blackouts and/or energy outages. However, fault detection and toleration actions in MEGs are still open research areas. The existing studies about hazard estimation are on a case-by-case basis [38–41]. Estimating fault propagation and analysing the consequences are major challenges for safety design verification. To implement a precise safety verification approach, it is vital to analyse and diagnose all hazard and fault events in the MEG and to study fault propagation scenarios. Figure 1 shows the MEG structure [4] which is utilized as a case study of MEG safety design.

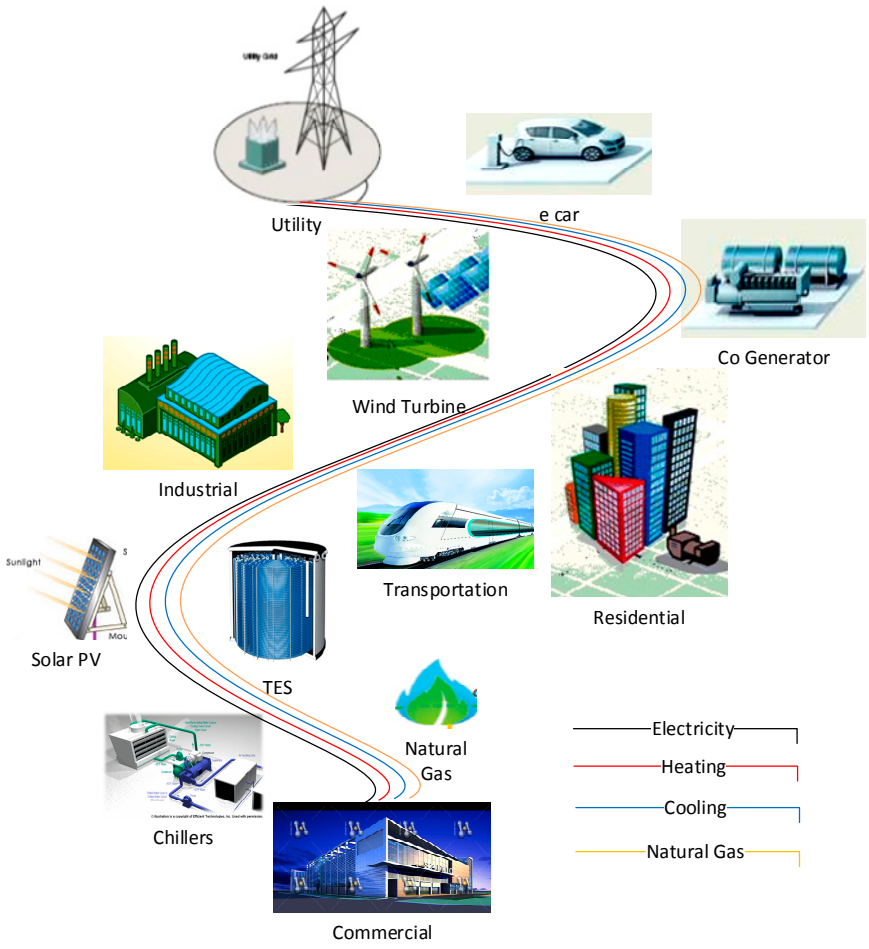

Figure 1. Proposed case study MEG model.

3. Research Methodology

The general objective of this research is to provide a methodology for safety design and verification of MEGs. This method offers a tool to achieve an accurate safety design of MEGs, by using developed hazard analysis and developed risk assessment evaluation methods, then implement the required IPLs, which consists of SIF and non-SIF systems, to achieve an acceptable safety tolerance margin. Finally, several hazard scenarios are studied to validate the MEG self-healing and resiliency performance. The research methodology is presented in Figure 2 and can be summarized as follows:

(1) Study hazards and estimate risks of a MEG such as hazards in electricity, heating, cooling, transportation sectors and hazards due to natural phenomena.
(2) Rank the hazard events based on the hazard level then prioritize them from most to least significant.
(3) Estimate MEG risks for all identified scenarios using developed fault tree analysis, and propose safety performance indicators for safety evaluation
(4) Study and develop IPLs for MEG safety design and evaluate SIL using developed *LOPA* analysis

Hence, the propsed safety technique can be projected on different MEG configurations with minor refinment to fit the new MEG configration.

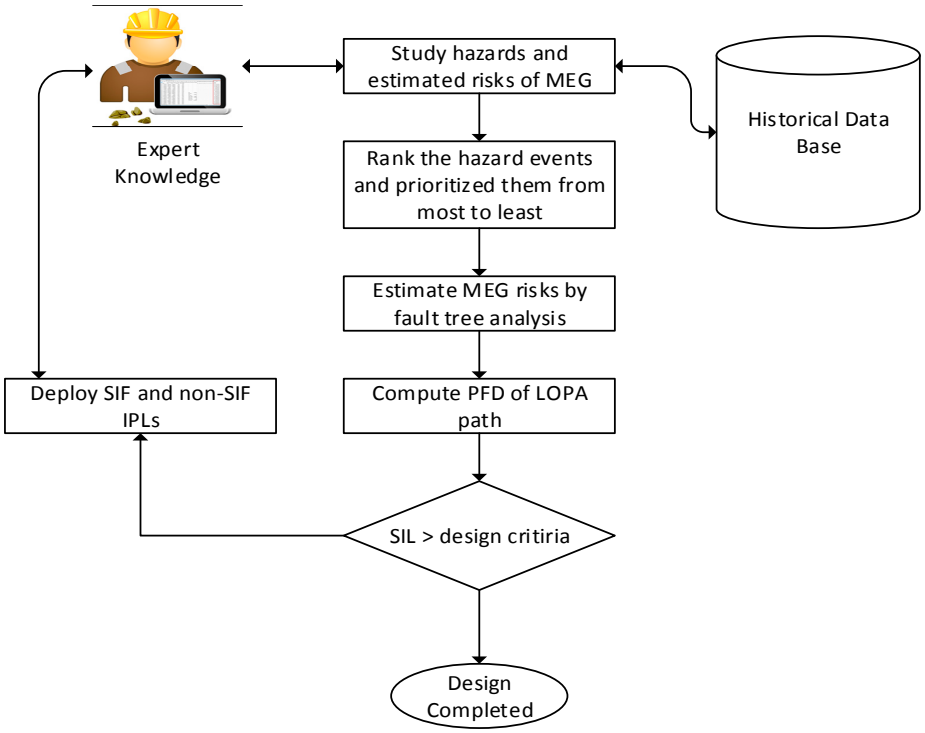

Figure 2. The research methodology.

3.1. Hazard and Risk Analysis Techniques for MEGs

The hazard matrix is an effective methodology used in risk analysis. The first use of risk matrix was in 1973 [42]. The hazard matrix has the ability to visualize and rank the hazard event based on its risk level. Therefore, it is an effective tool for risk analysis and decision making.

The MEG foundation design in this research does not use inherent safeguard protection layers. Table 1 shows the major hazards that threaten the MEG system in electrical, cooling, heating, natural gas and transportation grids, and it suggests the correspondent remedy actions to eliminate the negative impacts, and subsequently to avoid risks of failure or blackout.

Table 1. Excerpt list of hazards in MEG.

SI	Grid Type	Hazard Mode	Hazard Event	Severity	Frequency	Probability	Avoidance	Class	Hazard Level		Hazard Rank	Adverse Effects/Consequences	Action (Remedial, Prevention or Mitigation)	Proposed Solutions and IPLs
			SCORE	*1 = Negligible* *2 = Marginal* *3 = Critical* *4 = Catastrophic*	*1 = Less* *2 = yearly* *3 = Monthly* *4 = Weekly* *5 = Daily*	*1 = Negligible* *2 = Rarely* *3 = Possible* *4 = Likely* *5 = Common*	*1 = Likely* *3 = Possible* *5 = Impossible*	*3–4 = Very Low* *5–7 = Low* *8–10 = Moderate* *11–13 = High* *14–15 = Extremely High*	*HL* = S*C	*1 = Low* *2 = Moderate* *3 = High*	*Higher rank means higher risk*	(1) On Human (2) On Facility (3) On Environment		
1	Electrical MEG	Power Blackout	Over load (above the grid capability)	4	3	3	5	11	44	H	24	(1) Demand not Served (DNS) (2) Overheated transmission and distribution cables, Asset Damage, fire and power blackout (3) Fire cause CO_2 Emission	1—Upgrade grid capacity 2—Shift on-peak power demand 3—Dynamic grid mapping based on load demand and priority	1—Intelligent Energy Storage System (super capacitor, Fly Wheel, TES and pumped hydro, or hydrogen storage. 2—Intelligent Fault Tolerant Controller. 3—Ranking the loads as per its prioritization level.
2			MEG has lack of DER	4	3	3	3	9	36	H	16	(1) Interruption on service (2) Power interruption and/or blackout (3) Lack of DER = more demand on Fossil fuel generators which cause Emission	High dynamic performance from the distributed power and energy system by • Store off-peak power production for using at on-peak demand • Utilize Gas Generator • Connect to Capital Grid (Utility)	1—Intelligent Energy Storage System (super capacitor, Fly Wheel, TES and pumped hydro, or hydrogen storage). 2—Load Following or dispatchable generator (fuel cells, micro-gas turbines, and hybrid fuel cell gas turbine systems) 3—Higher level Self-Healing Management Controller
3			Intermittency of on site renewable sources	3	5	5	3	13	39	H	18	(1) Disturbance on service (2) Intermittency and non-coincidence of power production (3) Lack of DER = more demand on Fossil fuel generators		
4			Integration of multi sources DERs	2	5	5	3	13	26	M	8	(1) Operation Failure of Sensitive Devices (2) Negative impacts on grid parameters such as active power (P), reactive power (Q), voltage (V), phase shift (α) and frequency (f). In other words, poor power quality (3) Excessive on Energy Resources and Emission	1—Full utilization of DERs to increase energy efficiency 2—Improve power quality 3—Enhance system stability	1—Advanced D-FACTS system on AC/DC MEG to achieve resilient MEG 2—Create Robust KPI parameters able to optimize feedback control coefficients
5			Faults in the power systems (generation, transmission or distribution) systems	4	2	4	5	11	44	H	25	(1) Unsatisfied condition for customers (2) Power failure and/or outage may cause loss of business and production (3) Fire cause CO_2 Emission	1—Isolate the minimal affected branch 2—Switch off and isolate the DERs allocated in the affected zone	1—Wide area monitoring and alarm systems 2—Utilizing numerical smart relays 3—Emergency Shutdown system ESD 4—Periodical testing and maintenance procedure
6			Utility grid failure	4	2	2	2	6	24	M	5	(1) Unsatisfied condition for customers (2) Power failure and/or outage may cause loss of business and production (3) More demand on Fossil fuel generators	1—Open the main switch gear (islanded mode) 2—Standby all available DERs 3—Reduce the load based on priority and power production availability	1—Monitoring and Alarm systems for Utility grid energy quality and status 2—Safety management controller dealing with hazards scenarios 3—Emergency Shutdown system ESD

Table 1. *Cont.*

7		Solar Farm Outage	Solar Panel output drops by 60 MW in a 15 min.	4	3	4	3	10	40	H	19	(1) Breakers could trip leaving customers without electric power. (2) Voltage on the grid could drop and frequency of main generators could change (3) Increase the demand on coal-fired generators	1—Store off-peak power production for using at on-peak demand 2—Dynamic grid mapping based on load demand and priority	1—Adopt advanced power storage units such as super capacitor
8			Feeder circuit disconnects from substation	1	5	5	3	13	13	M	2	(1) The customer can no longer sell electricity to utility grid (2) Feeder circuit voltage could get out of phase with the grid (3) Increase the demand on coal-fired generators	1—Dynamic network based on load demand and priority 2—Reduce the load based on priority and power production availability	1—Intelligent Alarm systems for panel power quality and status 2—Adopt SIS management dealing with hazards scenarios
9			Short to ground on distribution grid	2	1	2	5	8	16	M	3	(1) Unsatisfied condition for customers (2) Equipment could be damaged, particularly transformers and capacitor banks. (3) Increase the demand on coal-fired generators	1—Dynamic network based on load demand and priority 2—Reduce the load based on priority and power production availability	1—Intelligent Alarm systems for panel power quality and status 2—Adopt SIS management dealing with hazards scenarios
10			Failure of DC to AC inverters	1	4	4	3	11	11	M	1	(1) The customer can no longer sell electricity to utility grid (2) Power failure and/or outage may cause loss of business and production (3) Increase the demand on coal-fired generators	1—Isolate the minimal affected branches 2—Switch off and isolate the affected inverters	1—Utilizing numerical smart relays 2—Periodical testing and maintenance procedure
11			High correlation of cooling demand with electricity demand	4	5	3	3	11	44	H	23	(1) Demand not served (2) Increase on-peak electricity demand could cause interruption and/or blackout (3) Increase demand on Fossil Fuel generation	Shift on-peak cooling demand to off-peak demand	1—Utilize TES tanks 2—Predictive energy management 3—Ranking the cooling demand as per its prioritization level
12	Cooling MEG	Cooling Outage	MEG cooling contingency load with lack of Chiller units	4	3	3	3	9	36	H	17	(1) Uncomfortable condition for human (2) Can't meet the on-peak cooling demand (3) Using individual A/C units lead to increase Global Worming	1—Isolate the affected chiller unit from both electrical and cooling network 2—Stand by all absorption chiller units for compensation purpose 3—Update the management control to reschedule storage strategies by store off-peak cooling production for using at on-peak demand	1—Utilize TES tanks 2—Intelligent contingency energy management (for emergency procedure) 3—Utilizing numerical smart valves
13			Faults in the Cooling system (Chiller, TES, Pumps or Pipes and valves) systems	4	2	4	5	11	44	H	22	(1) Unsatisfied condition for customers (2) Cooling energy failure may cause loss of business and production	1—Isolate the minimal affected branch 2—Switch off and isolate the cooling DERs allocated in the affected zone	1—Utilizing numerical smart meters 2—Emergency Shutdown system ESD 3—Periodical testing and maintenance procedure
14			Leak in the cooling pipe branch									(3) May cause pollution by liquid and gases spreads or by direct fire		

Table 1. *Cont.*

15			Cooling Overload	4	3	4	1	8	32	H	13	(1) Uncomfortable condition for human (2) Can't meet the on-peak cooling demand (3) Using individual A/C units lead to increase Global Worming	1—reduce the load as per priority index to match the production capacity 2—peak shave management for dispatchable loads to balance between power production and demand 3—Convert heating to cooling energy	1—Utilizing numerical smart meters 2—Emergency Shutdown system ESD 3—Utilize absorption chillers
16			Irregular hot-water demand	3	5	4	3	12	36	H	16	(1) Uncomfortable condition for human (2) Failure to meet the Hot water on-peak demand (3) Alternative heat sources like furnace produce emission	1—Store off-peak hot water production for using at on-peak demand	1—Utilize TES tanks 2—Predictive energy management
17	Heating MEG	Heating Outage	Thermal over load	4	2	2	3	7	28	M	9	(1) Uncomfortable condition for human (2) Failure to meet the Hot water on-peak demand (3) Alternative heat sources like furnace produce more emission	1—reduce the load as per priority index to match the production capacity 2—peak shave management for dispatchable loads to balance between power production and demand 3—discharge the thermal storage energy 4—switch off the absorption chillers	1—Utilizing numerical smart meters 2—Emergency Shutdown system ESD 3—Safety management controller dealing with hazards scenarios
18			Faults in the Heating system (Cogen, Boiler, TES, Pumps or Pipes and valves) systems	4	2	4	5	11	44	H	21	(1) Unsatisfied condition for customers (2) Heating energy failure may cause loss of business and production (3) Fire cause CO_2 Emission	1—isolate the minimal affected branch 2—switch off and isolate the thermal DERs allocated in the affected zone	1—Wide area monitoring and alarm systems 2—Emergency shutdown system ESD 3—Periodical testing and maintenance procedure
19			Loss of electrical boiler	4	2	2	3	7	28	M	10	(1) Unsatisfied condition for customers (2) Heating energy failure may cause loss of business and production (3) Alternative heat sources like furnace produce emission	1—Isolate the Electrical boiler from power and thermal networks 2—Standby Co-gen and gas boiler to cover the thermal deficiency 3—Update the management control to reschedule storage strategies	1—Wide area monitoring and alarm systems 2—Emergency shutdown system ESD 3—Periodical testing and maintenance procedure
20			Loss of gas boiler	4	2	2	3	7	28	M	11	(1) Unsatisfied condition for customers (2) Heating energy failure may cause loss of business and production (3) Alternative heat sources like furnace produce more emission	1—Isolate the Electrical boiler from power and thermal networks 2—Standby Co-gen and electrical boiler to cover the thermal deficiency 3—Update the management control to reschedule storage strategies	1—Wide area monitoring and alarm systems 2—Emergency shutdown system ESD 3—Periodical testing and maintenance procedure

Table 1. *Cont.*

21	Natural Gas	Natural Gas Outage	Gas Leak in Co-gen's feeder pipe	4	3	2	3	8	32	H	14	(1) Loss of life's, injury and suffocation	1—Close the affected branch 2—switch off and isolate the Co-gen from electrical and heating networks 3—switch to grid connected mode to cover the deficit in power production 4—standby boiler furnace to serve the thermal demand	1—Wide area monitoring and alarm systems 2—Emergency shutdown system ESD
			Gas Leak in boiler's feeder pipe	4	3	2	3	8	32	H	15	(2) Damage in assets and loss of business	1—Close the affected branch 2—switch off and isolate the gas boiler from gas and heating networks 3—standby electrical boiler to serve the thermal demand 4—switch to grid connected mode to cover the deficit in power production	
			Gas Leak in the Main Pipes	4	2	2	3	7	28	M	12	(3) Toxic gases and CO_2 Emission	1—Isolate the affected pipes 2—switch off all systems feed by affected pipes	
22	Transportation	Transportation Breakdown	Transportation energy demand	4	5	5	1	11	44	H	20	(1) Loss of life's , injury and suffocation (2) Failure in energy threaten the safety for properties and the public (3) Back-up engines works using fossil fuel which increase emission	1—Achieve energy management balance between transportation units and MEG for more reliability and security enhancement, reduced emissions and improved energy quality.	1—Energy storage system (super capacitor, flywheel, TES and pumped hydro, or hydrogen storage). 2—Following generator (fuel cells, micro-gas turbines, and hybrid fuel cell gas turbine systems) 3—Intelligent management controller
23	May affect all energy types	Natural Phenomenon	Earth quake	5	1	2	2	5	25	L	6	(1) Loss of life's, injury and delay (2) Failure in energy threaten the safety for properties and the public (3) Spreading the damages and may initiate new hazards	Isolate the affected area from the service	1—Intelligent Management Controller 2—Smart Relays and metering
24			Water flood	5	1	3	1	5	25	L	7	(1) Loss of life's, injury and delay (2) failure in energy threaten the safety for properties and the public (3) Spreading the damages and may initiate new hazards	Isolate the affected area from the service	1—Intelligent Management Controller 2—Smart Relays and metering
25			Thunder storm and lightning	5	1	2	1	4	20	L	4	(1) Loss of Life's , Injury and delay (2) Electrical devices might be damaged (3) Spreading of the damages and may initiate new hazards	Isolate the affected area from the service	1—Intelligent Management Controller 2—Smart Relays and metering

Each row in the hazard matrix (Table 1), describes a certain hazard in the MEG and shows relative statistical parameters such as consequence severity of hazard event, risk occurrence (i.e., frequency, probability and avoidance), hazard level, which derive from Equation (1) and hazard ranks which are assessed by experts. Furthermore, fault consequences and, suggested remedy actions and solutions are presented.

Generally, the hazard events are extracted from historical maintenance data and expert knowledge. Besides, the hazard occurrence parameters, i.e., frequency, probability and avoidance, can be evaluated from historical data or judged by expertise. Hence, the quantifying risk method used in this table was descried in Section 1.2 and shown in Equation (1):

$$Hazard\ Level\ (H_L) = S_i \times C_i \tag{1}$$

where, $C_i = (P_i + F_i + A_i)$ and S_i is the consequence severity of the hazard event, C_i is the class hazard event likelihood, P_i is the probability, F_i is the frequency, and A_i the ability for failure avoidance.

3.2. Safety Design, Risk Assessment and Protection Layers of MEG

MEG is commonly known as a dynamic structure system, with numerous operating conditions. Accordingly, it needs to improve adaptive protection strategies by means of intelligent control and supervisory units founded on safety measures and criteria.

The safety design of MEG is intended to improve rigidity of the energy system in the course of abnormal cases, as well as to avoid fault and damage propagation. The safety design approach can be realized by disturbing and isolating faulted or defected components in the MEG structure in addition to the inherent contribution of safety strategies on properties, the environment and public safeguards [43].

The IEC 61511 or ANSI/ISA-84.00.01-2004 standard describes safety instrumented system (SIS) as an instrumented system used to build one or more safety instrumented functions (SIF). SIS consists of groups of sensor(s), logic solver(s), and final element(s). Safety-related system is an alternative expression of SIS given by IEC 61508 [44].

Although, SIS is monitoring the process parameters, it enforces only when needed. Where control loop in basic process control system (BPCS) is utilized to keep process parameters within the tolerant marginal limits [45]. The proposed hazard analysis algorithm for MEG can be demonstrated in the following steps:

(1) Implement the MEG hazard table
(2) Rank the hazards based on the hazard level
(3) Filter the hazard events to eliminate hazards with low severity and high class as well as ones with high severity and low class.
(4) Prioritize the filtered hazard events
(5) Set out the feasible prevention and mitigation solutions to discuss the necessary action with the stakeholders.

In general, risk analysis idiom measures the hazardous conditions that appear during the operation intervals. Where the average time period between successive hazardous events is estimated to be over 10 years, if safety parameters are considered during the design process [46]. Accordingly, the SIS is passive during normal operation, and it may probably be only activated once or less during the ten year interval. Table 2 Illustrates the SIS operating conditions [47]. Fail-danger mode is the major hazard in the system, where despite the system operating ordinarily in this circumstance, the automatic protection of the SIS is not guarded, and there is no indication of that failure [48].

Table 2. Operating conditions of SIS.

SIS Operating Condition	Process	Protection Available	Failure Indication
Normal	Operating Normally	Yes	N/A
Fail-Safe	Falsely Operating	N/A	Yes
Fail-Danger	Operating Normally	No	Without Diagnosis

It is clearly defined that hazard analysis alone is not sufficient for the right decision. Where the hazards should be prioritized and discussed with the decision making team in light of the affordable level of fault consequences and the available budget dedicated for remedy actions. Figure 3 illustrates MEG hazards based on the hazardous level shown in Table 1. The following hazard events, shown in Table 3, have the highest hazard ranks, where they are allocated above the proposed catastrophic range "red curve"; those hazards must have priority in mitigation and prevention actions.

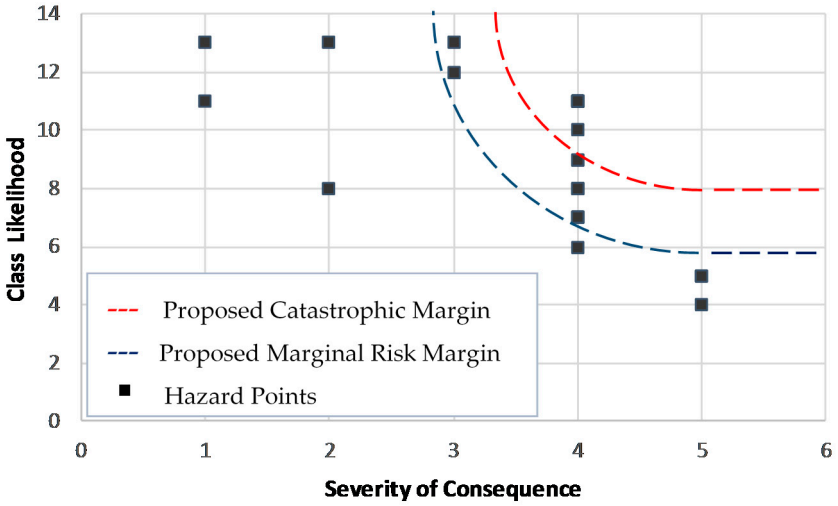

Figure 3. MEG hazards chart.

Table 3. Hazard events in catastrophic range.

SI	Hazard Mode	Hazard Events
1	Power blackout mode	Over load (above the grid capability)
2		Faults in the power systems (generation, transmission or distribution)
3	Solar farm outage	Solar panel output drops by 60 MW in 15 min time.
4	Cooling outage	Faults in the cooling system (chiller, TES, pumps or pipes and valves) systems
5		Leak in the cooling pipe branch
6		High correlation of cooling demand with electricity demand
7	Heating outage	Faults in the heating system (Cogen, boiler, TES, pumps or pipes and valves) systems
8	Transportation breakdown	Transportation energy demand

While the hazard events illustrated in Table 4 which have ranks between the proposed catastrophic margin "red curve" and marginal risk margin "blue curve" are medium priority in the remedy actions.

Table 4. Hazard events in marginal risk range.

SI	Hazard Mode	Hazard Events
1	Power blackout mode	Intermittency of on site renewable sources
2		MEG has lack of DER
3	Cooling outage	MEG cooling contingency load with lack of chiller units
4		Cooling overload
5	Heating outage	Irregular hot-water demand
6		Thermal over load
7		Loss of electrical boiler
8		Loss of gas boiler
9	Natural gas outage	Gas Leak in Co-gen's feeder pipe
10		Gas Leak in boiler's feeder pipe
11		Gas Leak in the main pipes

3.3. Safety Instrumented System Engineering Requirements

Nevertheless, a SIS is similar to a BPCS in numerous ways; the differences are found in the unique design, maintenance, and automated integrity requirements. Thus, in addition to the functional requirements of normal performance that are correlated with control system design, the following shall be considered for a SIS design [44]:

- Design to fail-safe
- Design diagnostics to detect fail-danger automatically
- Design manual test procedures to detect fail-danger
- Design to meet international and local standards

3.3.1. Safety Integrity Level

Safety integrity level (SIL) is an expression for the relative level of risk-reduction offered by a certain SIF, where SIL is an indication for system safety performance. IEC EN 61508 has defined by the relation of *PFD* (probability of failure on demand) and RRF (risk reduction factor) of low demand operation with SILs as shown in Table 5: [44].

Table 5. Relationship between average probabilities of failure on demand to safety integrity levels (SIL).

SIL	General Description	*PFD* Avg.	Risk Reduction Factor (RRF)	Availability (%)
4	Catastrophic community impact	10^{-4} to 10^{-5}	10,000 to 100,000	99.99 to 99.999
3	Employee and community impact	10^{-3} to 10^{-4}	1000 to 10,000	99.9 to 99.99
2	Major property and production impact; Possible injury to employee	10^{-2} to 10^{-3}	100 to 1000	99 to 99.9
1	Minor property and production impact	10^{-1} to 10^{-2}	10 to 100	90 to 99

3.3.2. Safety Instrumented Function

Safety instrumented function (SIF) is defined, by IEC 61511, as "safety function with a specified safety integrity level which is necessary to achieve functional safety" [49]. Safety function can be illustrated as "function to be implemented by a SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event." [16].

3.4. Fault Tree for MEG

Time to Failure (T) is one of the most important static parameters in safety engineering. It can be used to derive another important measurement, known as failure rate. The real-time failure rate is generally obtained by counting the number of failures per interval unit time for a selected quantity of identical components:

$$\lambda(t) = Failure\ Rate = \frac{Failures\ per\ time\ unit}{Quantity\ Exposed},\ \forall\ T > t \geq 0 \tag{2}$$

where, t refers to the operation time line, reliability is obtained by $R(t) = e^{-\lambda t}$, probability of failure on demand is obtained by $F(t) = 1 - e^{-\lambda t} \approx \lambda t$ and mean time to failure is obtained by $MTTF = 1/\lambda$.

The fault tree technique is widely used to present probability combinations. This technique starts with the definition of an "undesirable event", generally a process failure of some type. Then, the technique determines all the hazard events and the combinations of events that outcome in the undesirable event. Therefore, the fault tree is useful in modeling failure roots for a specific failure mode. Different failure modes can be presented by means of different undesirable events in different specific fault trees. Figure 4 illustrates a developed fault tree analysis for MEG. The top event is a probability of failure on demand (*PFD*) for a MEG blackout. The developed method offers a clear means to present multiple failure modes. The following equation evaluates *PFD* for a selected MEG [50]:

$$F(MEG) = F(Electrical\ Blackout) + F(Cooling\ Outage) + F(Heating\ Outage) \tag{3}$$

where:

- $F(Electrical\ Blackout) = F(Conventinal\ Grid\ Blackout) \times F(Renew.\ Blackout) \times F(Co-gen) \times F(TES) \times F(Manag.)$
- $F(Cooling\ Outage) = 3 \times F(Chiller) \times F(Co-gen) \times F(TES) \times F(Manag.)$
- $F(Heating\ Outage) = F(Co-gen) \times F(Boiler) \times F(TES) \times F(Manag.)$
- $F(Conventinal\ Grid\ Blackout) = F(Gen.) \times F(Transformer) \times F(Transmission\ Line)$
- $F(Renew) = F(PV) \times F(WT)$
- $F(PV) = F(Inverter) \times F(Panels) \times F(C.B) \times F(Ctrl)$
- $F(WT) = F(Pitches) \times F(Ctrl)F(C.B.) \times F(Motor)$

The *PFD* associated with each individual system in MEG can be demonstrated from a historical operation database and engineering experience. *PFDs* for selected individual components were shown in Tables 6 and 7.

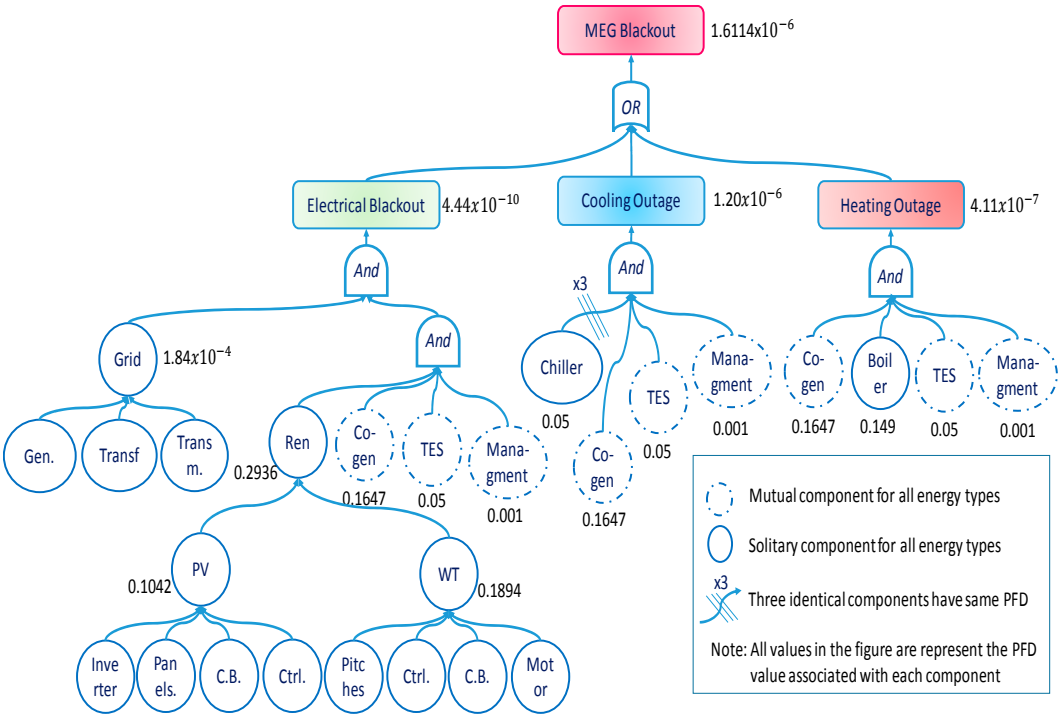

Figure 4. Fault tree analysis of MEG blackout top event hazard.

Table 6. Failure rate and repair time [51].

Type	Failure Rate (f/year)	Reliability $e^{-\lambda T}$	*PFD* $1 - e^{-\lambda T}$	Repair Time (h)
Solar Panel	0.11	0.8958	0.1042	72
Wind Turbine	0.21	0.8106	0.1894	60
Co-generator	0.18	0.8353	0.1647	12
Capital grid	0.000184	0.9998	0.000184	n/a
Chiller Unit	n/a	0.95 [52]	0.05	n/a
Fuel Cell	0.11	0.8958	0.1042	72
Battery	0.22	0.8025	0.1975	60
Micro Turbine/HRSG	0.16	0.8521	0.1479	16

Table 7. Typical outage rate for a consumer [53].

Contributor	Minutes/Year	%
Generation/transmission	0.5	0.5
132 KV	2.3	2.4
66 KV and 33 KV	8	8.3
11KV and 6.6KV	58.8	60.7
Low voltage	11.5	11.9
Scheduled shutdown	15.7	16.2
Total	96.8	100

The probability of an energy blackout for the MEG can be illustrated by compensating the individual component failure rates in Equation (5). It shows that the top event risk reduced 10^{-4} times by utilizing the proposed IPL and SIF components, discussed in Section 3.5, where the *PFD* became 1.6114×10^{-6} while it was originally 0.1992 for the conventional energy grids.

3.5. Independent Protection Layers and Layer of Protection Analysis

The independent protection layer (IPL) can be demarcated as a system, device, or action that can prevent the process from transferring to undesired consequence scenarios. It must be independent from the initiated event or the action of any other layer of protection linked with the scenario. The essential characteristics of IPL can be summarized as follows:

- Potential ability on suppressing the propagation of fault consequence, if the IPL functions as intended
- Auditable capability, where it assumed effective in terms of statistical validation of risk indices (by documentation, review or testing)

The layer of protection analysis (*LOPA*) is developed to determine whether the selected IPLs are sufficient in tolerating certain risks and suppressing the hazard of consequence scenarios [54]. Each IPL has its own *PFD*:

$$PFD = p_n,\ n \text{ indicates the layer level} \tag{4}$$

where the *PFD* value has a direct impact on system resiliency, as declared on the *LOPA* path Equation:

$$LOPA\ path = fn = \left(\prod_{i=1}^{i=n-1} p_i \right) \times f_0 \tag{5}$$

The IPLs shown in Figure 5 were proposed to mitigate the MEG's most hazardous events mentioned in Table 3. These IPLs are required to tolerate the hazard of losing energy in the MEG, by utilizing co-generators, TES, and supervisory fault-tolerant predictive energy management control. Consequently, utilizing the IPLs realizes the concurrent goals of increasing the energy availability, improving the production quality/cost, and reducing the gas emissions. Details of the proposed IPLs in this study are as follows:

➢ IPL-1 Co-generators to overcome the lack of power production at peak hours and to cope with the intermittency of renewable resources.

➢ IPL-2 Thermal energy storage as an effective tool for MEG operation due to the following advantages:

(A) Reshaping the energy profile by reserving the off-peak production to be used at on-peak demand hours.

(B) Centralized infrastructure where large thermal reservoirs provide flexibility to manage cooling dynamics, as well as lower emissions and energy failure risks.

➢ IPL-3 Supervisory fault-tolerant energy management (FTEM) controllers play a primary role the MEG reliability, where management of distributed resources near the renewable energy source is the most effective means of decreasing penetration of renewable resources.

➢ IPL-4 Safety alarm system is an important SIF layer, where its main role is to monitor the healthy status of the MEG and to provide real time information about the fault type and location, in case of a fault event.

➢ IPL-5 Emergency shutdown system (ESD) is a paramount SIF layer due to its ability in mitigating the consequences of the fault event when the above IPLs are unable to prevent the fault propagation.

Several combinations of different IPLs can be suggested to augment MEG resiliency. The following are examples of IPLs:

- MEG Storage system (E/T/C): energy storage units are classified based on their technology, the following are the most popular energy storages: batteries, super capacitors, flywheels, hydro tanks, thermal energy storage and superconducting magnetic energy storage

- Prime mover: co-generators, fuel cells, micro gas turbines, geothermal resources and hybrid turbine systems
- Intelligent control systems for normal operation to ensure rigid performance
- Smart energy asset management for both sources and load within the MEG boundary
- Emergency control for resilient systems on abnormal cases
- Risk assessment platform and alarm system
- MEG safety shutdown and restoration systems
- Upper-level centralized / decentralized MEG management with utilities grids.

These IPLs can be presented in future studies to explore different techniques and compare their performances on the MEGs resiliency.

LOPA shows reduction on system risk level from 0.199054, SIL-0, for the conventional energy grid to 1.611×10^{-6}, higher than SIL-4, with the selected non-SIF IPLs, i.e., Co-gen, TES and managements control.

By adding the selected SIF IPLs as shown in Figure 5, *LOPA* path value can be dramatically reduced by 10^{-4}, as defined using Equation (7); where $LOPA = f_5 = 0.119 \times 0.1647 \times 0.05 \times 0.001 \times 0.1 \times 0.01 = 1.6114 \times 10^{-10}$ which further increases further the margin beyond SIL-4 level.

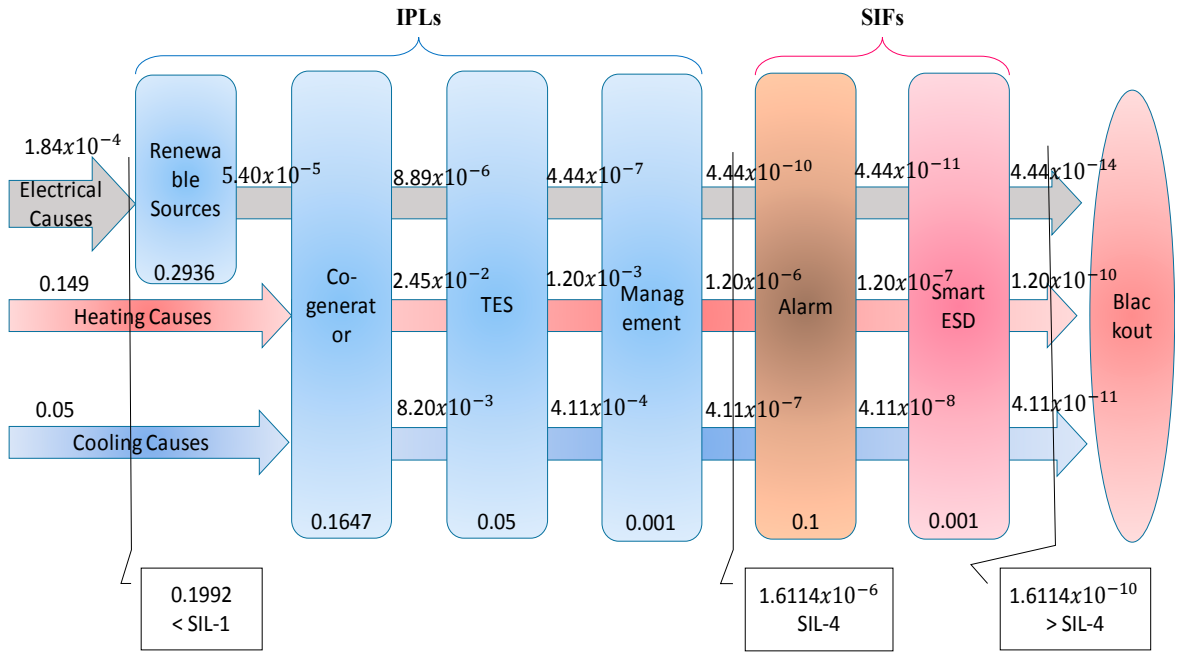

Figure 5. Proposed *LOPA* path diagram for MEG.

4. Summary

In this paper, a study for safety design and risk analysis within the MEG was developed to achieve a resilient MEG design and implementation. Framework for the safety design methodology was presented and discussed. A developed hazard matrix was proposed for MEG, and a hazard analysis algorithm was contributed to assist the decision maker in prioritizing hazardous events. Afterward, advanced fault tree and *LOPA* were utilized to estimate the risk reduction and SIL parameter for incorporating selected IPLs in the MEG. Selected SIF and non-SIF IPLs were utilized to achieve a resilient MEG by increasing SIL. Extremely high hazards, that have either high severity with low class or high class with low severity, were eliminated, to focus on the major effective hazards and to propose suitable IPLs to prevent their consequences. The results showing that the proposed non-SIF protection layers reduce the risk of MEG blackout by 10^{-5} and the proposed SIF protection layers offer

another 10^{-4} to the safety performance of the original MEG. In light of the promising results of this research, it can be affirmed that the proposed methodology offers an effective safety tool for MEG design and verification. The proposed tool can be widely utilized in design and verification of large complex systems.

Author Contributions: The main idea proposed in this paper was conceived and designed by Hossam A. Gabbar and Yahya Koraz; Hossam A. Gabbar and Yahya Koraz gave experiment design; Yahya Koraz performed verification experiments; Hossam A. Gabbar and Yahya Koraz wrote this paper.

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

References

1. Koraz, Y.; Gabbar, H.A. Hierarchical Safety Control for Micro Energy Grids using adaptive neuro-fuzzy decision making method. In Proceedings of the IEEE International Conference on Smart Energy Grid Engineering, Oshawa, ON, Canada, 21–24 August 2016; pp. 131–136.
2. Gabbar, H. Design and Planning Support Tool for Interconnected Micro Energy Grids. *Br. J. Appl. Sci. Technol.* **2016**, *12*, 1–15. [CrossRef]
3. Zhang, J.; Yang, Z.; Zhou, Q. Reliability Assessment for Micro-grid with Multi-Energy Demand. In Proceedings of the China international Conference on Electricity Distribution, Shenzhen, China, 23–26 September 2014; pp. 23–26.
4. Gabbar, H.A.; Koraz, Y. Safety Design of Resilient Micro Energy Grids. In *Smart Energy Grid Engineering*, 1st ed.; Elsevier: Amsterdam, The Netherlands; Academic Press: Cambridge, MA, USA, 2017; pp. 101–150.
5. Dieck-Assad, G.; Masada, Y. Optimal Set-point Scheduling in A Boiler-turbine System. *IEEE Trans. Energy Convers.* **1987**, *EC-2*, 388–395. [CrossRef]
6. Garduno-ramirez, R.; Lee, K.Y. Multiobjective Optimal Power Plant Operation Through Coordinate Control with Pressure Set Point Scheduling. *IEEE Trans. Energy Convers.* **2001**, *16*, 115–122. [CrossRef]
7. Chandan, V.; Jabbari, F.; Brouwer, J.; Akrotirianakis, I.; Chakraborty, A.; Alleyne, A.; Do, A.; Jin, B.; Jabbari, F.; Brouwer, J. Modeling and optimization of a combined cooling, heating and power plant system. In Proceedings of the 2012 American Control Conference (ACC), Montreal, QC, Canada, 27–29 June 2012; pp. 3069–3074.
8. Saponara, S.; Bacchillone, T. Network architecture, security issues, and hardware implementation of a home area network for smart grid. *J. Comput. Netw. Commun.* **2012**. [CrossRef]
9. Chan, D.; Cameron, M.; Yoon, Y. Implementation of micro energy grid: A case study of a sustainable community in China. *Energy Build.* **2017**, *139*, 719–731. [CrossRef]
10. Telecom, K.; Korea, S. Korea Micro Energy Grid Technology The use case of the First-town in Sejong. In Proceedings of the Netwwork Operation Management Symposum (APNOMS), 15th Asia-Pacific, Hiroshima, Japan, 25–27 September 2013.
11. Song, G.; Chen, H.; Guo, B. A layered fault tree model for reliability evaluation of smart grids. *Energies* **2014**, *7*, 4835–4857. [CrossRef]
12. Chaves, A.; Terry Bahill, A. Comparison of risk analysis approaches and a case study of the risk of incorporating solar photovoltaic systems into a commercial electric power grid. *Syst. Eng.* **2014**, *17*, 89–111. [CrossRef]
13. Bahill, A.T. Diogenes, a process for identifying unintended consequences. *Syst. Eng.* **2012**, *15*, 287–306. [CrossRef]
14. Agrawal, A.B.; Barker, K.; Haimes, Y.Y. Adaptive multiplayer approach for risk-based decision-making: 2006 Virginia Gubernatorial Inauguration. *Syst. Eng.* **2011**, *14*, 455–470. [CrossRef]
15. Bahill, A.T.; Karnavas, W.J. Risk analysis of a pinewood derby: A case study. *Syst. Eng.* **2000**, *3*, 143–155. [CrossRef]
16. Saponara, S.; Fanucci, L.; Bernardo, F.; Falciani, A. Predictive Diagnosis of High-Power Transformer Faults by Networking Vibration Measuring Nodes with Integrated Signal Processing. *IEEE Trans. Instrum. Meas.* **2016**, *65*, 1749–1760. [CrossRef]
17. Saponara, S. Distributed measuring system for predictive diagnosis of uninterruptible power supplies in safety-critical applications. *Energies* **2016**, *9*, 327. [CrossRef]

18. Zidan, A.; Khairalla, M.; Abdrabou, A.M.; Khalifa, T.; Shaban, K.; Abdrabou, A.; El Shatshat, R.; Gaouda, A.M. Fault Detection, Isolation, and Service Restoration in Distribution Systems: State-of-the-Art and Future Trends. *IEEE Trans. Smart Grid* **2016**. [CrossRef]
19. Costantino, N.; Serventi, R.; Tinfena, F.; D'Abramo, P.; Chassard, P.; Tisserand, P.; Saponara, S.; Fanucci, L. Design and test of an HV-CMOS intelligent power switch with integrated protections and self-diagnostic for harsh automotive applications. *IEEE Trans. Ind. Electron.* **2011**, *58*, 2715–2727. [CrossRef]
20. Friedl, W.; Fickert, L.; Schmautzer, E.; Obkircher, C. Safety and reliability for smart-, micro-and islanded grids. In Proceedings of the CIRED Seminar 2008: SmartGrids for Distribution, Frankfurt, Germany, 23–24 June 2008; p. 15.
21. Nikkhajoei, H.; Lasseter, R.H. Microgrid Protection. In Proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 24–28 June 2007; pp. 1–6.
22. Hooshyar, A.; Iravani, R. Microgrid Protection. *Proc. IEEE* **2017**, *105*, 1332–1353. [CrossRef]
23. Lee, W.S.; Kang, S.H. Protection for distributed generations in the DC micro-grid. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 5–7 December 2011; pp. 1–5.
24. Lai, K.; Illindala, M.S.; Haj-ahmed, M.A. Comprehensive Protection Strategy for an Islanded Microgrid Using Intelligent Relays. *IEEE Trans. Ind. Appl.* **2017**, *53*, 47–55. [CrossRef]
25. Zhao, X.X.; Xia, M.C.; He, X.H.; Zhou, Y. Study on protection scheme for micro-grid with mobile energy storage units. *Procedia Eng.* **2011**, *16*, 192–197.
26. Deng, W.; Pei, W.; Shen, Z.; Zhao, Z.; Qu, H. Adaptive micro-grid operation based on IEC 61850. *Energies* **2015**, *8*, 4455–4475. [CrossRef]
27. Arnauld, A. *Logic, or, the Art of Thinking: Containing, Besides Common Rules, Several New Observations Appropriate for Forming Judgment*; Cambridge University Press: New York, NY, USA, 1996.
28. Haimes, Y.Y. *Risk Modeling, Assessment, and Management*, 4th ed.; John Wiley & Sons. Inc.: Hoboken, NJ, USA, 2015.
29. Bahill, A.T. Design and Testing of an Illuminance Management System. *ITEA J.* **2010**, *31*, 63–89.
30. Daniels, J.; Werner, P.W.; Bahill, A.T. Quantitative methods for tradeoff analyses. *Syst. Eng.* **2001**, *4*, 190–212. [CrossRef]
31. Cooper, J.A. Soft Mathematical Aggregation in Safety Assessment and Decision Analysis. In Proceedings of the System Safety Society Conference, Orlando, FL, USA, 16–21 August 1999.
32. Kerzner, H. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, 11th ed.; John Wiley & Sons, Inc.: New York, NY, USA, 2013.
33. Bahill, A.T.; Daniels, J. Correction to Quantitative Methods for Tradeoff Analyses. *Syst. Eng.* **2005**, *8*, 93. [CrossRef]
34. Ben-Asher, J.Z. Development Program Risk Assessment Based on Utility Theory. *Risk Manag.* **2008**, *10*, 285–299. [CrossRef]
35. Carbone, T.; Tippett, D. Project risk management using the project risk FMEA. *J. Eng. Manag.* **2004**, *16*, 1–8. [CrossRef]
36. McManus, T.N. *Management of Hazardous Energy Deactivation, De-Energization, Isolation, and Lockout*; CRC Press: Boca Raton, FL, USA; Taylor & Francis Group: New York, NY, USA, 2013.
37. Ma, T.; Wu, J.; Hao, L. Energy flow modeling and optimal operation analysis of the micro energy grid based on energy hub. *Energy Convers. Manag.* **2017**, *133*, 292–306. [CrossRef]
38. Abdelsamad, S.F.; Morsi, W.G.; Sidhu, T.S. Impact of wind-based distributed generation on electric energy in distribution systems embedded with electric vehicles. *IEEE Trans. Sustain. Energy* **2015**, *6*, 79–87. [CrossRef]
39. Zio, E.; Golea, L.R. Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements. *Reliab. Eng. Syst. Saf.* **2012**, *101*, 67–74. [CrossRef]
40. Liu, Z.; Liu, Y.; Zhang, D.; Cai, B.; Zheng, C. Fault diagnosis for a solar assisted heat pump system under incomplete data and expert knowledge. *Energy* **2015**, *87*, 41–48. [CrossRef]
41. Zhao, Y.; Xiao, F.; Wang, S. An intelligent chiller fault detection and diagnosis methodology using Bayesian belief network. *Energy Build.* **2013**, *57*, 278–288. [CrossRef]
42. US Department of Defense. *Military Standard 882B System Safety Program Requirements*; US Department of Defense: Washington, DC, USA, 1984. Available online: http://sunnyday.mit.edu/safety-club/882b.htm (accessed on 8 August 2017).

43. Pradhan, D.K.; Mathew, J.; Shafik, R. *Energy-Efficient Fault-Tolerant Systems*; Springer Publishing Company: New York, NY, USA, 2014.
44. Goble, W.M.; Cheddie, H. *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*; ISA-The Instrumentation, Systems, and Automation Society: Research Triangle Park, NC, USA, 2005.
45. Wolter, K. *Stochastic Models for Fault Tolerance: Restart, Rejuvenation and Checkpointing*; Springer: New York, NY, USA, 2010.
46. Abbasi, A.R.; Seifi, A.R. Considering cost and reliability in electrical and thermal distribution networks reinforcement planning. *Energy* **2015**, *84*, 25–35. [CrossRef]
47. Piesik, E.; Śliwiński, M.; Barnert, T. Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 259–272. [CrossRef]
48. Dubrova, E. *Fault-Tolerant Design*; Springer: Berlin, Germany, 2013; pp. 55–65.
49. Baybutt, P. Risk tolerance criteria and the IEC 61511/ISA 84 standard on safety instrumented systems. *Process Saf. Prog.* **2013**, *32*, 307–310. [CrossRef]
50. Koraz, Y.; Gabbar, H.A.; Gabbar, A. Risk Analysis and Self-Healing Approach for Resilient Interconnect Micro Energy Grids. *Sustain. Cities Soc.* **2017**, *32*, 638–653. [CrossRef]
51. Danesh, H.K.-Z.H. Microgrid Energy Management System: A Study of Reliability and Economic Issues. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–5.
52. Schroeder, A. Modeling storage and demand management in power distribution grids. *Appl. Energy* **2011**, *88*, 4700–4712. [CrossRef]
53. Eeh Power Systems Laboratory. UCTE System Adequacy Forecast. 2007. Available online: https://www.entsoe.eu/news-events/former-associations/ucte/system-adequacy/Pages/default.aspx (accessed on 8 August 2017).
54. Islam, M.R.; Gabbar, H.A. Study of Micro Grid Safety & Protection Strategies with Control System Infrastructures. *Smart Grid Renew. Energy* **2012**, *3*, 1–9.