2013

Security Evaluation of Substation Network Architectures

Pingal Raj Sapkota
Michigan Technological University

Follow this and additional works at: https://digitalcommons.mtu.edu/etds
Part of the Electrical and Computer Engineering Commons

SECURITY EVALUATION OF SUBSTATION NETWORK ARCHITECTURES

By

Pingal Sapkota

A THESIS

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In Electrical Engineering

MICHIGAN TECHNOLOGICAL UNIVERSITY

2013

This thesis has been approved in partial fulfillment for the requirements for the Degree of MASTER OF SCIENCE in Electrical Engineering.

Department of Electrical and Computer Engineering

Thesis Advisor:	*Dr. Chee-Wooi Ten*
Committee Member:	*Dr. Zhuo Feng*
Committee Member:	*Dr. Laura E. Brown*
Department Chair:	*Dr. Daniel Fuhrman*

Contents

List of Figures

List of Tables

Acknowledgements

I would like to express my deepest appreciation to Dr. Chee-Wooi Ten who has been very supportive, motivating, and inspiring throughout this journey. Without his constant help and guidance this thesis would not have been possible.

I would like to thank my committee members, Dr. Zhuo Feng and Dr. Laura E. Brown for taking time to go through my work and provide valuable suggestions.

In addition, many thanks to my colleagues Md. Rashiduzzaman Bulbul, Guna Bharati, and Niraj Dhital for their help when I needed it. I would also like to thank Mr. Andrew Ginter from Waterfall Security Solutions, Mr. Terrance Ingoldsby from Amenaza Technologies, and National Science Foundation for their support.

Last but not the least, a very special thank you to my family, specially my parents and my beautiful wife Pranita Sharma, for being very supportive and understanding throughout this journey.

List of Abbreviations

λ	Failure rate
μ	Repair rate
A	Availability
B	Breach of trust indicator
BCU	Bay control unit
C	Cost indicator
CNS	Corporate network server
DCP	Digital control panel
DHC	Dual-homed computer
DHS	Dual-homed server
DMZ	Demilitarized zone
DUM	Dial-up modem
EI	Ethernet interface
ESW	Ethernet switch
FW	Firewall
HMI	Human machine interface
IPC	Industrial personal computer
MTTF	Mean time to failure
MTTFF	Mean time to first failure
N	Noticeability indicator
NCCS	Network control center server
P, Ps	Probability of success
R	Reliability
RX	Receiver of unidirectional gateway
T	Technical ability indicator
TX	Transmitter of unidirectional gateway
V	Vulnerability index

Abstract

In recent years, security of industrial control systems has been the main research focus due to the potential cyber-attacks that can impact the physical operations. As a result of these risks, there has been an urgent need to establish a stronger security protection against these threats. Conventional firewalls with stateful rules can be implemented in the critical cyberinfrastructure environment which might require constant updates. Despite the ongoing effort to maintain the rules, the protection mechanism does not restrict malicious data flows and it poses the greater risk of potential intrusion occurrence.

The contributions of this thesis are motivated by the aforementioned issues which include a systematic investigation of attack-related scenarios within a substation network in a reliable sense. The proposed work is two-fold: (i) *system architecture evaluation* and (ii) *construction of attack tree* for a substation network. Cyber-system reliability remains one of the important factors in determining the system bottleneck for investment planning and maintenance. It determines the longevity of the system operational period with or without any disruption. First, a complete enumeration of existing implementation is exhaustively identified with existing communication architectures (bidirectional) and new ones with strictly unidirectional. A detailed modeling of the extended 10 system architectures has been evaluated. Next, attack tree modeling for potential substation threats is formulated. This quantifies the potential risks for possible attack scenarios within a network or from the external networks. The analytical models proposed in this thesis can serve as a fundamental development that can be further researched.

1 Introduction

The chapter starts with the recent development of communication protocols in power industry and discusses their impact on cybersecurity of the substation infrastructure. The chapter describes how conventional boundary protection mechanisms such as firewall fail to provide a complete security measure to the networks of critical cyber-assets as well as its limitations. This chapter also describes the required changes to improve boundary protection of critical infrastructures. First, general cyber-attack performed by intruders and different types of communication that facilitate such attacks are discussed. Then, unidirectional communication gateway and how it can improve the cybersecurity of the substation infrastructure is identified. Finally, a brief review of previous work carried out in this area is elaborated in the end of this chapter.

1.1 Evolution of Power Communication Infrastructure

Power infrastructure is going through a revolutionary change due to the growing energy demands, new standards in regulation, and growing dependency on IP-based communication. These paradigm changes are reflected in the infrastructure and operation of the substation network. The development of communication protocols such as IEC61850 and intelligent electronic devices (IEDs) are some examples of such advancement. Traditionally segragated, simple and proprietary networks are now evolving into more complex, widely-connected, and interdependent networks [1]. Although these networks are isolated from the public domain, the implementation of IP-based communication infrastructure poses a risk for cyber-intruder to gain access to the critical cyber-assets [2]. While such transformation has made the interoperability between vendors possible and provided additional functionalities such as remote control and remote accessibility, such transition has also exposed to larger pool of untrusted networks and individuals. An unauthorized user with sophisticated knowledge and tools can successfully penetrate into a substation network and exploit the security framework [3–5]. To implement an in-depth defensive protection of the cyberinfrastructure, weaknesses and access points shall first be identified. There have been research on boundary protection of transmission line systems. An integrated relay based protection scheme and the theory of boundary protection for high voltage transmission lines connected to a substation is described [6, 7]. In computer security, the protection scheme is divided in layers and these layers have a aggregate effect for the defense against external attacks [8].

Cybersecurity of power grid control network, one of the nation's critical infrastructures, has received higher level of attention in United States due to the regulation of North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) [9, 10]. NERC-CIP standards have made a significant impact on utilities that deploy IP-based communication infrastructures, which include critical cyber-assets that can have the capability to control the physical facilities of the grid [11]. However, most efforts have been focused on compliance of government regulation; establishing a framework to systematically assess the component/system vulnerabilities for a critical cyber- network has been limited [9]. NERC-CIP standards only include minimum protection requirements, and compliance with the standards does not guarantee adequate level of system security to critical cyber-assets [12]. Stakeholders including utilities, vendors, and system integrators remain committed to establish a specific business case for their system deployment in addition to complying with the government cybersecurity mandate.

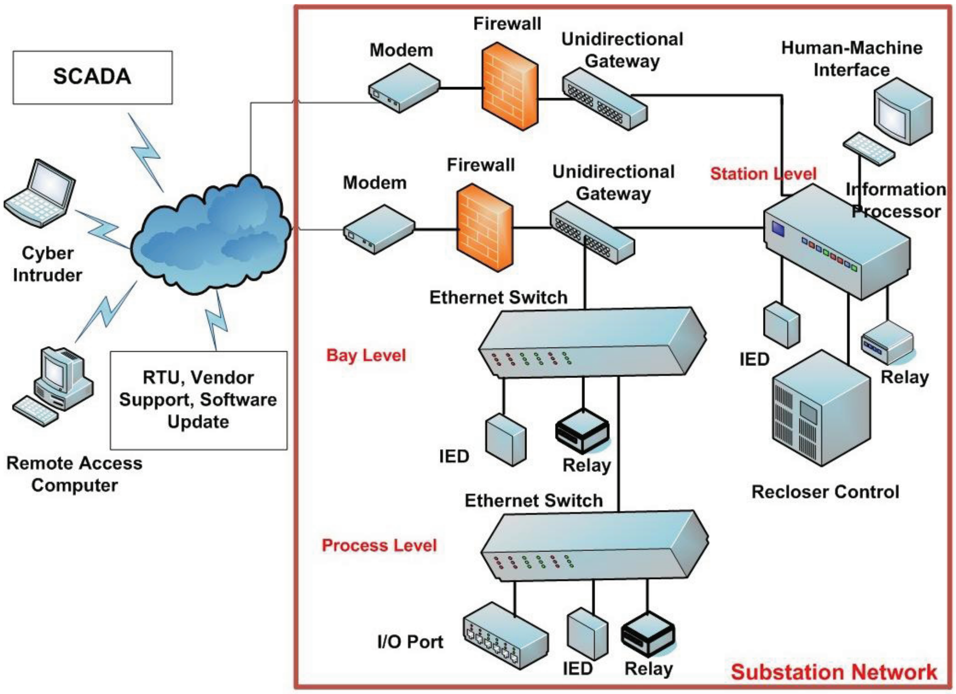


Figure 1: Substation Network

This thesis contributes to the development of analytical technique to identify cybersecurity vulnerability in a substation network. Basic characteristics of network security are integrity, confidentiality, availability, and controllability of information flow [13]. Confidentiality, integrity, and availability (CIA) are the three factors that are used to evaluate the security of any cyber-system. Reliability and attack tree method are useful in measuring some of these factors. In one hand, reliability measures availability as well as integrity of the system. On the other hand, attack tree analyzes the confidentiality and integrity of the system. These two methods together can evaluate the all three factors of CIA.

The system model for the substation network is depicted in Fig. 1. Security risk can arise from network access points shown in the model. These access points can be connected by vendors/users via corporate or supervisory control and data acquisition (SCADA) networks to maintain the field devices in substation network. Security threats to network security include malicious attacks by insiders or outsiders that can be executed by the vulnerabilities of loopholes in networking software or non-authorized access due to the poorly maintained access control list of the network users [13].

1.2 Firewall Technologies

Conventional firewalls are deployed in the industrial control environment to protect the critical infrastructure of the power grids that govern the physical conditions with control and monitoring capability. While these have been successfully implemented to filter the malicious packets between two networks, they are not designed to monitor the contents of packets flowing through them. As the firewall technology advances and new techniques are being developed, the algorithms of detecting anomaly in firewalls might not be effective due to its design and specification that can affect strategic planning and management of the firewall systems [13]. Misconfigured or incorrectly-planned firewall can result more hassle in maintaining them than the network without firewall deployment [14].

1.2.1 Firewall Limitations

Most conventional firewalls provide false sense of security as it only restricts the packets flowing through based on the strictly defined rules, which are extremely challenging to keep them up to date [15]. It is possible for outsiders to access the firewall-secured network by manipulating users and using high-level programming language. Most common type of firewall technology is based on packet filtering, which allows only specific types of data packets to transfer through security network. However, intruders can mask the source of incoming packets deceptively to make them appear as they were originated from one source which does not necessarily indicate the original location [14]. Another disadvantage of such technique is that intruders can execute an attack through a less-secure already-compromised access point to send the malicious packets.

Another type of boundary protection is application-based firewall that controls user authentication to the network [13]. With such firewall, the communication between internal and external hosts is not allowed under normal scenarios. However, if the external host is compromised by an attacker, the internal host or network can be a stepping stone for attackers to further explore new information for future hacking.

Proxy service has been recognized in corporate network that is implemented in the boundary level of a network. This restricts direct communication between internal and external hosts [14]. Both hosts communicate with the proxy servers instead of direct connection between the two systems. The role of proxy server is to relay the communication back and forth between the two. However, proxy systems can only be effective if there is a restriction in the network to prohibit direct communication between internal and external hosts [14]. If a direct communication is allowed to establish connections, then implementation of using proxy server is bypassed and it no longer provides the desired protection [14].

1.2.2 One-Way Communication

Restricting one way communication can drastically enhance the overall security compared with the conventional firewall deployment. This is due to the limitation of hardware capability that can only enable one way of packets flow which deters intrusion attempts and unauthorized access. This technology has been commercially promoted, *e.g.*, “The Pump” developed by Naval Research Laboratory and “Waterfall one way" developed by Waterfall Solutions [16, 17]. The senders and transmitters on both sides are defined with hardware requirements which physically restrict the data flow between the two networks in unidirectional manner. The hardware design of these “diodes” cannot allow data flows in the reverse direction [17].

1.3 Attack Footprints

Generally, intrusion to a network will require the following steps. First, the adversary would investigate to progress to the communication network through the access points (enumeration). Upon successful penetration, (s)he will continue to gather network information (learning and discovery). Once the attacker understands the control process and information that is connected to the instrumental of physical system, an attack can be planned to maximize the disruption [18]. This thesis emphasizes on the cyberdefense framework to analyze the existing architectures.

1.3.1 Possible Attack Pathways

For the outsider attack, there are two ways of accessing the control system network. One way is to go through the common path, which is through a network firewall. Another way is by bypassing the common path to establish a direct connection with the control system network. Therefore, when strengthening the protection level of the firewalls, it is important to enumerate all access points and ensure the "backdoors" access are completely eliminated.

1.3.2 Bypassing Security Framework

One of the most common ways to bypass the security framework is to directly connect with the modems that are attached to control center equipment [18]. Attackers will attempt every possible phone number in the area (prefix number of a utility) trying to connect to the modem. Another way is by connecting to Remote Terminal Units (RTU). Usually, modems and RTUs are configured with passwords. It is crucial that modems and RTUs are protected with passwords that cannot be easily guessed [18]. Additionally, vendors can have a direct communication link through dial-up modem in order for them to periodically upgrade the system or to maintain the system whenever required. Attackers can use this direct communication path to identify a possible intrusion path. As a defender, enumerating all possible direct points must be checked constantly to avoid any unauthorized intrusions.

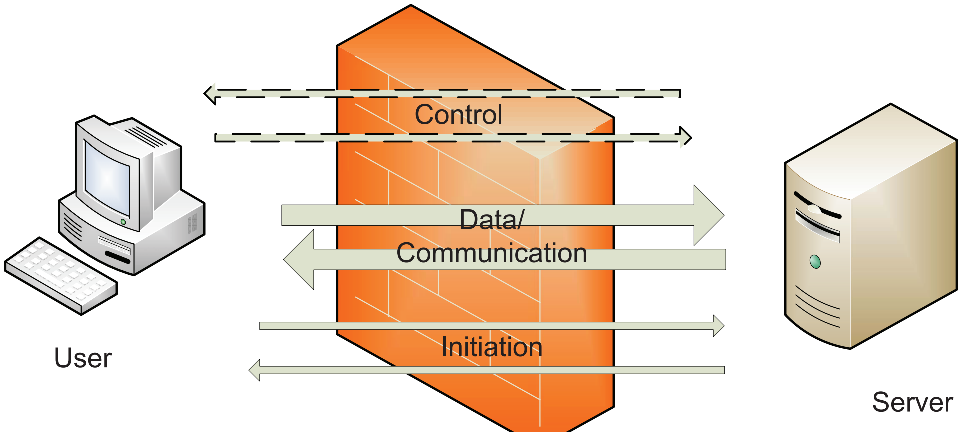


Figure 2: Bidirectional Communication

1.4 Types of Communication

Three different types of communication can take place through a firewall as depicted in Fig. 2. The first step is the connection establishment initiated by the external host with internal server. This is a bidirectional connection that can be established with the acknowledgement from the other party through through firewall. A unidirectional connection can be established only by deploying the hardware-restricted directional devices.

1.4.1 Bidirectional Communication

For a bidirectional communication, data flows are in both directions. An example of this would be the SCADA data that is sent from a substation network through RTUs to the control center. Another type of communication is the control action that is sent to the external host such as field worker to the control center or from vendor support to control center equipment. Risks with a bidirectional communication is that an intruder can mask malicious data and can send it through the firewall pretending to be sent from an authorized source such as RTU or vendor support. If the firewall cannot identify this as malicious, then the attacker will be able to obtain other critical information from these networks which can be useful to further plan for a cyber-attack.

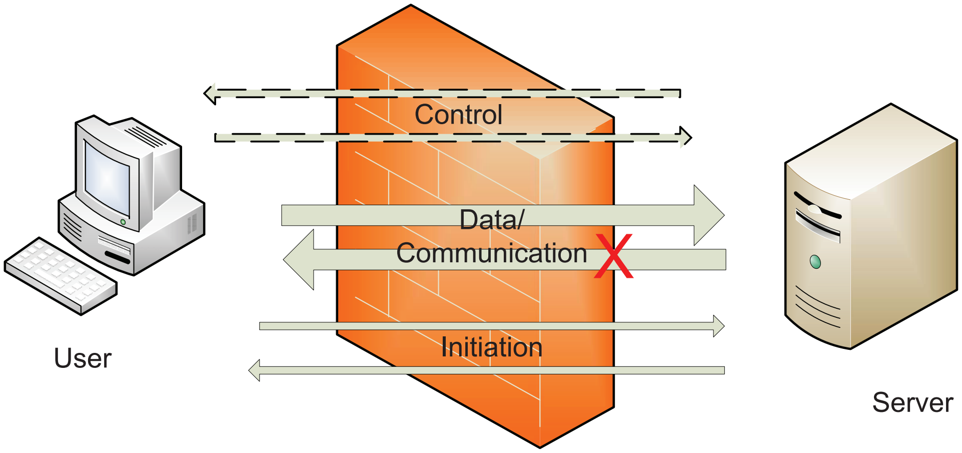


Figure 3: Partial Unidirectional Communication

1.4.2 Unidirectional Way

In a unidirectional communication, the information flows in from lower security level to higher security level and no backflow of data is possible [17, 19]. One-way communication can have different levels of enforcements, where one or more of the initiative, data, and control communications are restricted by the hardware design. There are several products in the market which are based on one-directional communication. Although the data transfer with such products is in one direction, the bidirectional communication has to be established first within the network before it is relayed to external network. This can be confusing as most one-way communication may still allow some kind of communication in reverse direction as depicted in Fig. 3. In this thesis, one-way communication shown in Fig. 4 [19] is discussed in three types of signals, *i.e.*, initiation, data, and control.

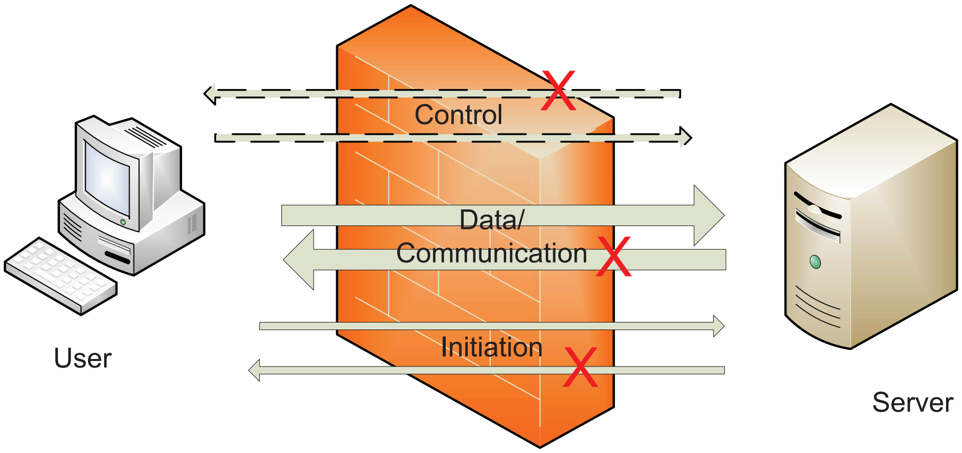


Figure 4: Complete Unidirectional Communication

1.4.3 Two Layers of Unidirectional Gateways

To improve the performance of unidirectional gateways, two layers of data diode can be architected, *i.e.*, 2 unidirectional gateways with one gateway at each side of the networks. This will improve the security enforcement since the data flows have to pass through two layers of filters instead. The use of two layers can practically limit the communication to almost null. The potential intrusion would be a highly unlikely scenario as the unidirectional communication restricts the external flow of the critical information. Specific industrial protocol software agent will work with the hardware to send the data to other side of network which does not require the acknowledgement of data received on the other side [17]. For any intrusion attempt, the attackers require an immediate response if the targeted hosts are responding in order to explore possibilities of access points. With this architecture, the attackers will not receive any information and cannot exploit new information.

1.5 Boundary Protection Within a Network

One-way communication is not designed to replace the boundary protection and other protection technologies that are used in the individual computers. Various software such as anti-virus programs and their updates are also critical to be used in substation hardened computers. Anti-virus software help in maintaining system integrity by protecting against malicious computer codes such as viruses and worms [20]. System Integrity checkers monitor any changes to important files that are critical to the substation network [20]. There has been increasing concern about using any protection software whether or not they should be updated regularly. System managers need to make sure that the communication takes place securely during such updates. The drawbacks are that each software patches may be at risk to break the existing software dependency due to the compatibility of other software modules.

1.6 Research Contributions

This proposed research explores a new tool in assessing system vulnerability. It identifies the vulnerable access points and various types of attacks in a substation network. Network architecture based on unidirectional gateways is designed to restrict any intrusion attempts to access a network. Attack tree modeling is developed for the substation network to demonstrate the vulnerability of each access point. Experimental results demonstrate that the new architectural design of unidirectional gateways in a substation network enhance the overall cybersecurity.

1.7 Remainder of This Thesis

The remainder of this thesis is organized as follows: Chapter 2 provides an overview of the substation-control center network and communication protocols used in the networks. Vulnerability in different network components is also highlighted in this chapter. Chapter 3 provides the reliability modeling of new substation architectural design. Chapter 4 analyzes the evaluation of attack tree for a substation cybersecurity. Results and analysis based on various attack scenarios are presented. Chapter 5 concludes with future research recommendations.

2 Modern Power Communication Framework

A "smart grid" concept has been introduced in recent years to provide an envisioned agenda to automate the energy configuration in an optimal manner. The legacy communication networks will be upgraded with IP-based communication infrastructure that can comprise of multiple mesh networks, where all the subnetworks combine to form a greater network with multiple gateways and all meters have access to other gateways [21]. Communication architecture for this envisioned network will be exclusively IP-based such as within a network and between other networks that form a wide area network (WAN) [22]. An early warning system against denial of service (DoS) attacks in the modern communication framework using Gaussian process is presented [23]. The proposed vision has increased interdependency with the telecommunication network [24]. For accurate risk analysis, information regarding all interdependent infrastructures is necessary. Risk prediction of the network requires complete knowledge of each infrastructure and modeling of each components of the network [25].

Remote control and management of systems, units, and functions are essential features of this vision [26,27]. The authors of [28] proposes a visual real-time monitoring system for remote operations of electrical substations. While such system provides high-level visual support for remote monitoring, successful intrusion into such system will provide attacker with high-level knowledge of the critical infrastructure. It appears that implementation of virtual private network (VPN) gateways to remote monitoring system has improved overall system security of the protected network [29].

2.1 Anomaly Detection in Substation-Control Center Networks

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are the more sophisticated boundary protection to improve the cybersecurity of power control networks [25]. Implementation of domain-specific anomaly detection in the networks remains in premature phase. Most experts in anomaly algorithms in the computer community have made decent progress in identifying network anomalies. A survey has been conducted to identify methods used in anomaly detection [30]. Some proposed iterative estimation of Hurst parameter for rapid detection, opportunistic sampling for classification of anomaly detection, and network intrusion detection with semantics-aware capability are presented in [31–33]. Data-driven technique based on the concept of symbolic dynamics and information theory is described in [34]. Data reconstruction based on detection of random anomaly with RX-detector is shown in [35]. A signal processing approach using statistical technique to detect network anomalies has been proposed in [36]. Some researchers propose an operational limits and effectiveness to conclude an intrusion [37]. There is an attempt to infer potential cyber-intrusion by extracting irregular information within a substation network [38].

2.2 Vulnerabilities of Power Communication Networks

Most architectures found in a substation network are established with multiple generations of proprietary and standardized software protocols. Commercial-off-the-self (COTS) products such as MS-Windows, web servers, browsers, and application databases are commonly used in these networks. Other COTS products commonly used are IT protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and eXtensible Markup Language (XML). Vulnerability in these COTS products will introduce existing vulnerabilities to substation networks. Similarly, network security breach in a control system of the substation can also arise from the local area network (LAN). LAN also provides remote access to control center and field devices. In addition, most substation devices have Ethernet ports that are used for connection to the IP-network. Similarly many legacy protocols such as Modbus, Distributed Network Protocol 3.0 (DNP3), Inter-control Center Communications Protocol (ICCP) are IP-based. [39] attempts to propose an information architecture for future power system communication. There are new security threats arising due to all of these technologies. The following subsections describe the main components of a typical substation-control center networks:

2.2.1 Substation Network

Substation network consists of two layers, *i.e.,* process level and bay level comprising of protective relays, actuators, and merging units. This network is connected to external network through firewall protection. It is also connected to user interfaces of the substation level. Substation network is connected to control center network through another set of firewall protection. An attack can be launched from inside the network by insiders.

2.2.2 SCADA Systems

SCADA System has the salient features of monitoring and control for the industrial control systems that is deployed in a private protected environment. SCADA obtains measurements from the network topology and RTUs that are located in geographically expansive area. SCADA is connected to the secured substation network through dial-up modems or VPNs. Most SCADA instrumental information produces a massive amount of data between control center and substations. It is challenging to have dispatchers filter out the information messages that can focus on high priority issues of the physical health [40]. The cyber-attacks upon SCADA systems can be classified into two categories: intelligent or brute-force attacks. Brute-force attacks are carried by the attacker who is not an expertise in the specific domain of industrial control systems. Attacker with subsequent knowledge and capability of specific domain would maximize the attack consequence with their intelligence [41].

There are various standards and guidelines for designing the SCADA system. IEEE standard for SCADA and automation system provides guidance about designing and specification of SCADA automation system [42]. IEEE P1711 is a trial-use standard for cryptographic protocol for cybersecurity of substation serial links [43] and its tutorial for implementing IEEE P1711 is discussed [44]. It is used for communication between SCADA master and IEDs.

2.2.3 User Interface of Industrial Hardened Computers

User interfaces are located in the substation network as well as control center network. This can be attackers' interests for two obvious reasons. First, the user interfaces can have meaningful and easy-to-understand messages about the working of the system. An attacker can gain the understanding of the network through these messages. Second, attacker can mask malicious data packets and make them look like they are sent through a user. External attackers can use these interfaces to launch an attack.

2.2.4 Control Center Networks

Control center networks are protected by another layer of firewall from substation network. Control center has the most critical information and the ultimate goal of an cyber-intruder would be to get access to this area of the network. This is why the control center should have extra layer of protection. The goal is to stop any attempt of an unauthorized intruder to get access to this part of the network. However, control center can be directly connected to field workers or vendor support through dial up modems. It is extremely important that these direct connections are either avoided or made secure to avoid any intrusion through this path.

2.2.5 Cyber-Intruders

Cyber-intruders are the unauthorized individuals or networks that are outsiders to the substation network, who try to access the secure network with the intent of obtaining critical information or damaging the system. Cyber-intruders lie outside of the protective network and attempt to break the communication protocol of a secured network.

2.3 Security Threats

In general, there are two types of security threats to a substation network. First type is called untargeted threat in which attacker is not interested in a particular data or resources, rather attacker may only be looking to access the vulnerable devices without any specific motive. Worms and viruses are most common type of such threats. Other untargeted threats are unpatched systems, unauthorized access to system devices, and insecure connections. Employees can also be a part of such threats knowingly or without knowing by accidental misconfigurations and improper use of workstations.

Second type of threat is called targeted threat. Organized crimes and terrorists attacks are common motives behind such attacks. It is important to note that Al- Qaeda computers in Afghanistan were found to contain documents on SCADA systems [45]. These attacks pose more danger to the substation infrastructure because the attacker has a specific motive and will repeatedly pursue it. Use of botnets for distributed denial-of-service (DDOS) and extortion, and zero-day attacks fall into this category. Rival companies with the intention of manipulating the market can carry an industrial espionage which is also considered targeted attacks. Discontent insiders with password access can also launch targeted attacks to vent their frustration with the company. Mostly, power system is operated in N-1 contingency and loss of one single unit such as generation or transmission line can be compensated by rerouting or using backup generation. However, targeted cyber-attacks can cause the system to go beyond N-1 condition [46].

2.3.1 Within a Substation

Modern substations are deployed with devices such as sensors,IEDs , information processors, data servers, and IP-based communication infrastructure as shown in Fig. 5. IED is a family of devices that are based on microprocessors and includes relays, actuators, servers, gateways, and information processor. They are used for monitoring and control of other

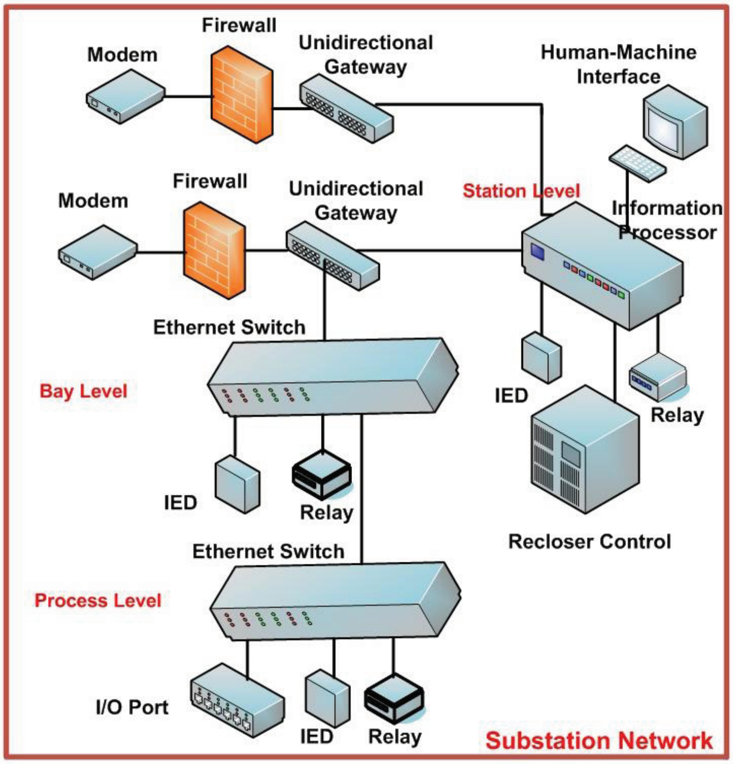


Figure 5: Within a Substation

substation devices and remote field devices, operations including power flow analysis, protection of the breakers, transformers, etc., and metering of the real-time data. Relays are essential devices present in a substation which collect measurements of current and voltage transformers (CTs and VTs) and check system parameters in real-time. Programmable Logic controllers (PLCs) communicate with relays, RTUs, reclosers, and satellite clocks. They are used for event reporting, operation and control of substation, remote control of field devices, and metering. Ethernet switches are used for communicating with SCADA system. Information processor present in the substation integrates information from wide variety of microprocessor devices and support functions such as high-speed data and logic processing and protocol conversion. Remote input/output has ports for monitoring external contacts and supports integration of SCADA, relays, and PLCs. Other devices present in a substation are satellite clocks, Ethernet gateway, VPN end-points, and firewall devices.

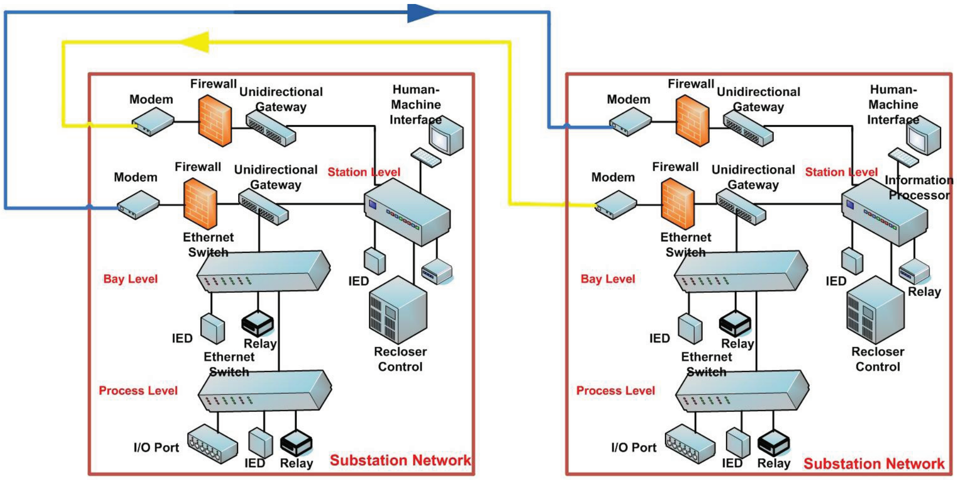


Figure 6: Substation to Substation Communication

2.3.2 Between Substations

In the current state of art, inter-substation communication occurs through various technologies such as power line, satellite, optical fiber, wireless, and wireless network sensors [47]. There are different types of substations present in the power system, namely generation, transmission, and distribution substations. Substations are connected to other substations for various purposes. For example, generation substations are connected to transmission and distribution substations for supplying power. Traditionally, substation to substation communication happens for power transfer and protection. However, with the advancement of substation technology and the ability of the substations to carry out more functions, substation to substation communication have larger objectives and functions. Physically connected substations share equipment such as breakers, relays, transformers between them. Data and status of these devices are exchanged between the substations through the communication network. Simultaneous failure of interconnected substation networks may cause cascading failures. During cascading failures, disturbance propagates through the interconnected substation networks resulting in large area blackout. Attackers may be interested to cause this phenomenon by attacking interconnected substations through the communication network. Fig. 6 shows the connection between two substations.

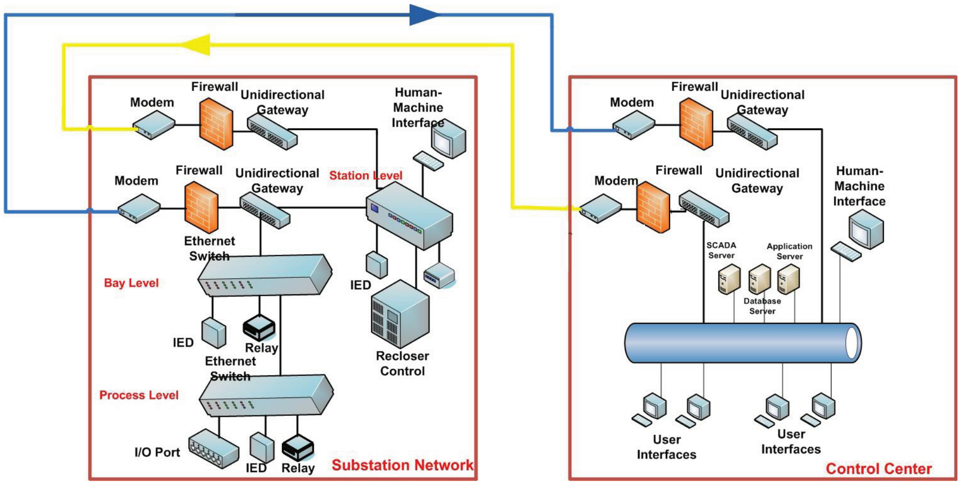


Figure 7: Substation to Control Center Communication

2.3.3 Between Control Center and Substations

Fig. 7 shows the communication network between a control center and a substation.Control center lies in the center of the power system and controls substation, generation, transmission, and distribution systems. Control centers communicate with substations for protection and operation. Substation networks are continuously monitored by the control center and such monitoring is essential for regular operation of the substation network. In an event of failure of a control center, there is a back-up control center which takes over the functions of the primary control center. Their operation is essential and are responsible for power system reliability and stability.

In the past, control centers were established to processes the data from the SCADA system. This was necessary as the substations did not have the processing capability. In addition, control centers handled the operation, logical testing, and time synchronization of the available data in the absence of satellite clocks. Since not every substation was equipped with RTUs, state estimator in substations provided the missing data. It was also responsible for creating sequence of events and analyzing disturbances. Probably the only common goal substation and control center shared was time synchronization of RTU measurements .

At present, because of the large amount of data coming from synchrophasors and due to higher accuracy requirements for the data, control center are not capable of processing all the data on their own. Therefore, substations are being equipped with more devices with advanced communication capability that can perform most functions of a traditional control center. Substation devices are integrated into Programmable Automation Controller (PAC) which is capable of processing data in the scale of control centers [48]. However, this does not decrease the role of a control center; rather the interaction between substation and control centers is even increased. Synchrophasors measurements from substations are sent to the control center, which feeds the information back to the substation for protection functions. Wide area control and protection is based on the interaction of substations and control centers.

With the development of IEC61850 substation communication protocols, modern communication system check all measurements and status from substation data processing and transfer them to the control center as messages containing added information [48]. Data processing in both substation and control center allows comparison of measurement to improve the quality of data. Control center operators can warn local substation operators about any consistencies. In addition, control centers acknowledge any problems that could not be solved at the substation level. The changing roles of substations and control centers have brought increased interaction between these two entities. This has also given more opportunities for cyber-attackers to intrude the system.

Usually, substations are separated from control center network by a firewall connection. Such firewall is configured to allow TCP/IP traffic to IP-enabled devices in the substation/control center through specific ports. Such traffic is accumulated at a gateway device and this gateway device communicates with the individual devices within the substation. The direct communication with the individual devices is usually prohibited. However, such traffic only includes device diagnostics and configuration data. The traffic containing the operational data is communicated through serial ports. But there are some utilities that use TCP/IP for the operational data that are coming from SCADA system. Although rare, few utilities also have remote access to the SCADA and such connection happen through a firewall.

Control centers are also connected to regional Independent System Operator (ISO) and corporate network. Usually ISO communication happen through a firewall managed by ISO and allows only the TCP/IP traffic. ICCP packets from utility are embedded into TCP/IP traffic by an ICCP gateway and are sent through the firewall. Generally, the backflow of traffic from the ISO connection is not allowed. So the security risks from such connection is minimal. However, communication practices with the corporate network differs from utility to utility. In such connection, the primary traffic across the firewall is for remote access and data transfer. Some utilities have the database and web servers inside the control center network, however others have it in the corporate network. The communication happens through a firewall and is configured to allow users to these databases and servers. Network vulnerability can arise through such connection.

2.3.4 Between Primary and Backup Control Centers

Backup control centers are designed to carry out the functions of the primary control center in any events of major failure or unexpected emergency. The objective is to provide the uninterrupted data and functionality with no impact on performance at all time. The concept of two control center architecture has become more evident due to seemingly unavoidable nationwide cascading failures such as blackout of 2003. During normal operation, primary and back-up control centers exchange operational database and critical application files. Primary and backup control centers operate in same environment, use identical data and applications, follow identical operational procedures, and contain identical devices and user interfaces [49]. Generally, these two entities are connected through corporate LAN

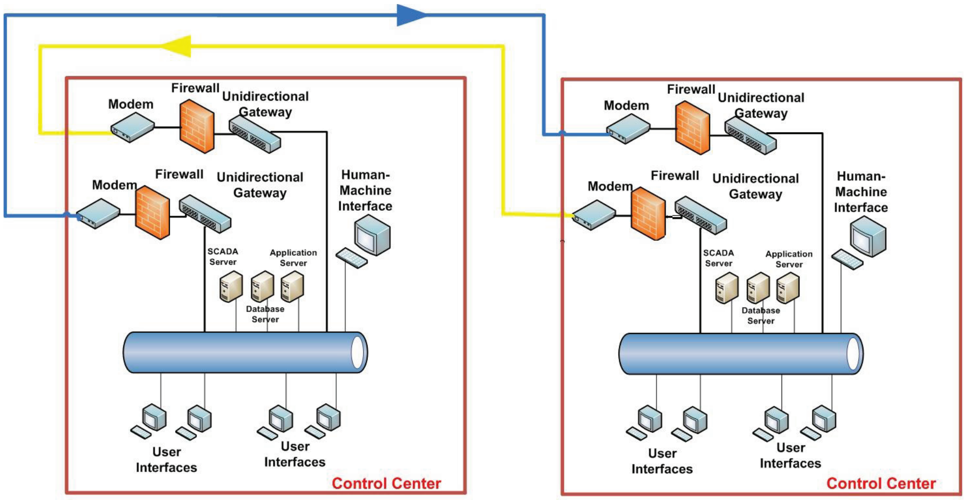


Figure 8: Inter-Control Center Communication

and web servers and over the TCP/IP or Ethernet. If an attacker successfully penetrates a control center, (s)he may also penetrate the back-up control center applying the same techniques. Fig. 8 shows the communication network between two control centers.

2.4 Communication Protocols

IEDs have become the common features of substations since the last two decades. Most recent IEDs are sophisticated devices that are capable of communicating with number of vendors which will ultimately lead to the inter-operability between devices from different vendors [50]. Because of these IEDs, the substation automation which relies on the standardization of communication and development of common protocols have become possible.

2.4.1 Modbus

Modbus is a communication protocol used for transmitting information from control devices to the data management system and main controller [51]. In the substation network, Modbus is used to transfer data from RTU to the supervisory computer of the SCADA system. Functions like remote control and automated monitoring are supported by Modbus [51].

2.4.2 DNP3

DNP3 developed around the same time as utility communications architecture (UCA), which later became known as IEC60870. Previous protocols were proprietary and used larger bandwidths. DNP3 limited the amount of bandwidth used. During the development of DNP3, application layers on protocols were not valued as important in SCADA system, so DNP3 used as few layers as possible. DNP3 uses only the three layers of open systems interconnection (OSI) model: physical layer, data link, and application layers [52]. The effectiveness of cyber-attacks against DNP3 increases rapidly if the DNP3 is embedded over TCP/IP [53]. In such case, attacks that are launched against TCP/IP can be used against DNP3.

2.4.3 ICCP

Modern power grid is widely interconnected. Utilities need to exchange information such as measurements, status and control data, scheduling, energy accounting, and operator messages. ICCP is the standardized communication across such interconnections connecting utilities for real time data exchange. In the United States, ICCP is used for interconnecting regional system operator to the transmission, distribution, and generation utilities. It uses manufacturing messaging specification (MMS) and UCA specifications to encourage multiple vendors to implement the common protocol [54]. ICCP is commonly used over TCP/IP or Ethernet cable and are vulnerable to attacks that are generally used against TCP/IP.

2.4.4 OPC

Object Linking and Embedding for Process Control (OPC) acts as the common platform for Windows based softwares and process control hardware to communicate with each other [51]. Because of this function of OPC, hardware and software development can be treated as separate processes, allowing manufacturers to focus on just one aspect [51].

Three things are considered while standardizing the communication: 1) functions that include protection, control, and monitoring, 2) services that include the transferring of different types of data and, 3) protocols which depend upon the development of technology [55]. Functions and services of substation networks are more or less the same since decades. What changes is the technology which makes the development of new communication protocols. Data transfers in bit sequences and these bit sequences depend upon protocol. When technology changes, protocol changes and bit sequences need to be adjusted to the new protocol. Substation automation system (SAS) can not be replaced every time such technological changes happen. IEC61850 separates functions, and services from the protocol and maps them to the new protocol [55].

2.4.5 Attacks Through a Firewall

Firewalls are the most common defense boundary technologies for industrial cybersecurity. In addition to firewalls, industrial systems have other threat management systems such as anti-virus, intrusion detection, intrusion prevention, anti-spam, and web filtering. Firewalls are deployed in layers. The corporate network is separated from control network by one or more firewalls. Generally, demilitarized zone (DMZ) is present between such networks. DMZ acts as an intermediary between such networks. Communication usually happens in two folds, DMZ relaying the communication. Layers of host and network protection lie between networks and DMZ. Following are the most common methods for an attacker to pass through the firewall.

- Phishing/Spear-Phishing
  Phishing is a common way of attacking a corporate network. Attacker sends an email directing user to open a website hoping to get user's password. Spear-phishing is a

targeted attack where the attacker does a research and finds out a vulnerable individual, usually someone with a public face and finds out his/her activities such as a meeting or a conference (s)he is attending. Attacker then forges an email impersonating someone from the meeting. In this way, attacker makes more convincing approach to directing the victim to opening the attachment or clicking on the provided link. Corporate network is vulnerable to such type of attack, but control network usually have defense mechanisms that would prevent such attack. If not prevented attacker usually drops a worm into the machine allowing remote control of the user's machine.

- Steal a password
  Stealing a password is another way of getting through a firewall. There are software programs designed to work on the target computer as a method of keystroke logging which is primarily used to steal passwords. Keystroke logging tracks the keys on victim's keyboard when the victim types a password.

- Compromise a domain controller:
  Most control-center networks are designed to run on their own even in the absence of external networks or inputs. However, usually passwords are stored in the servers of the corporate network. In the event of an employee leaving the company, the company revokes all the passwords or accesses of the employee from the system. This is obtained by updating the domain controller. If the attacker has already compromised the domain controller and created a new account, such account will also be updated, giving attacker all the accesses to the control network.

- Attack exposed servers
  If a server on the control network is exposed to the attacker or is compromised by the attacker, every ports of the server are vulnerable to an attack. Attacker can then launch attacks such as structured query language (SQL) injection, buffer overflow, DoS, or password attacks.

- Attack industrial control system (ICS) clients via compromised servers
  Attacks can also arise from clients or trusted networks via compromised servers. In such cases, attacker do not need to initiate communication, it is initiated by the host or client themselves. Once the connection is established, attacker sends compromised files or data packets across the network.

- Session hijacking/man in the middle
  For man-in-the-middle attacks, attacker fakes session ID usually through a fake Wifi access port or hacked domain name system (DNS) server. Attacker does not initiate or participate in the communication directly but inserts new commands to existing communication session. Address resolution protocol (ARP) spoofing on LAN is a common type of man-in-the middle attack.

- Piggy-Back on VPN
  Most corporate networks have VPN accesses for trusted users. However, the attacker may have compromised the machines of such users. VPNs generally have broad rules

allowing the user with wide area of accesses. Attacker can exploit such accesses allowing the attacker to remotely interact with the corporate network.

- Firewall vulnerability
  Firewalls are software and can have deficiencies such as bugs and manufacturer defects. Manufacturers of these firewalls may also be controlled by a nation or terrorist organizations with specific interests or intrusion goals. Although firewalls have rules that only allow access to essential connections, there are usually large numbers of essential connections in a large enterprise such as a utility company. Such manufacturing or operating defects may be exploited by the attacker to gain access through the firewall.

- Errors and omissions
  Over time security holes may have been created through the firewall. For example, when a plant is down, the plant manager opens a firewall rule to allow access to the maintenance staffs through the firewall to work on the problem. There may be large number of such activities over time. If the operator forgets to revoke such accesses once the maintenance is over, there may be large number security holes created through the firewall. Attacker can exploit these security holes to intrude through the firewall into the control network.

- Forge an IP address
  Usually firewalls allow accesses only to the requests coming from recognized IP addresses. By forging an IP address to impersonate the trusted address, an attacker can take over an existing session or initiate a new session.

2.5 Quantifying Security Features

To study the security level of a network, anomaly detection methods need to be employed at different network access points [56]. Traffic distribution features need to be tracked for anomaly detection [32]. Most common of such features are:

- Source IP address
- Destination IP address
- Source access point
- Targeted destination point
- Data size

These features need to be evaluated in a quantitative way to determine the vulnerability of the network. Degree of vulnerability will depend on the successful data packets that reach the targeted destination with minimum trials or in shortest time. The vulnerability goes down when the communication architecture is changed from bidirectional to unidirectional. More quantitatively, the following features are indicative of the cybersecurity of the network. Together, quantifying these features will be useful in anomaly detection and identifying the degree of network vulnerability to cyber-attacks.

- Time to access
  For an cyber-attacker to launch a successful attack, the communication has to be established first between the server and the host, so that the malicious data packets can be sent. Longer it takes for this communication to establish, longer it takes to launch a successful attack.

- Connection Establishment
  In a bidirectional or partial unidirectional communication, when a successful communication is established, a response is received by the attackers of the successful initiation. In a complete unidirectional communication, they will not receive such acknowledgment and hence will have no knowledge of their intrusion attempt. This will largely discourage the attackers to launch any intrusion attempt.

- Number of Successful Intrusions
  A successful connection of the attacker with the internal host is considered a successful intrusion. This is the first step in launching an cyber-attack.

- Total Number of Attempts
  External intruder without an expertise of the network will attempt many tries to establish a successful intrusion. Instead of the attacker trying itself, a computer program will attempt these trials. The probability of the successful intrusion increases as faster the next attempt can be made. However, if the firewall is capped to allow only so many connection requests in a certain time, it can effectively block a rapid inflow of such requests.

- Volume of Data Flow
  Once a communication is established, the attacker would want to send data packets. These data packets can be malicious and intended to inflict damage or they will be intended to extract useful information from the network which will help the attacker to launch an even powerful attack. Either way, limiting the flow rate of such data packets can prevent damage it can cause. Some attackers will be interested to flood the data more than the servers can handle and thus stop the operation, limiting data flow rate will avoid such flooding.

- Spreading of Malicious Packets
  Most malicious data packets are designed to reproduce rapidly once they reach the target. Anomaly detection should keep track of any such rapidly increasing data. In case of any successful intrusions, this will allow the operators to take actions before any cyber-attack is launched. Fast propagating malware does not need a bidirectional data flow, rather one packet can be sufficient to inflict the malware in the network [17].

3 Reliability Evaluation of Substation Architectures

There is no single metric or multiple metrics that can assess cybersecurity accurately. NERC and regulators emphasize on compliance metrics but the system is not completely immune from cyber-attacks. There is a need for predictive metric to measure the cybersecurity of a network. Three factors are considered important measures of security: confidentiality, integrity, and availability. On a power system network, confidentiality is the least important because most of the power system data consists of voltage and current measurements which do not have much significance on the attacker. But modifying such measurements can create system imbalance and lead to failures in the system. Thus, integrity of data is an important measure. The main goal of the power delivery system is to adequately supply uninterrupted power to its consumers. Therefore, availability or reliability is the most important measure of power system cybersecurity.

In this chapter, reliability analysis is used to measure the reliability of 9 common substation architectures and a new architecture based on unidirectional gateways. All these architectures consist of a corporate network and a control network. Within the substation network, four different topologies are considered: star, ring, simple cascading, and redundant cascading [57]. Failure and repair rates of individual components are used to calculate the overall reliability of each architecture. Typical SAS components such as human machine interface (HMI), industrial personal computer (IPC), network control center server (NCCS), Ethernet switch (ESW), Ethernet interface (EI), and optical fiber (OPT) are included in the substation topology [57,58]. Two models, repairable and non-repairable models are considered for the analysis. In a repairable model, components can be repaired after each failure and do not need replacement. While in non-repairable model, components can not be repaired but have to be replaced after the first failure. Availability, reliability, mean time to failure (MTTF), and mean time to first failure (MTTFF) are evaluated for each architecture using repair and failure rates. In addition, sensitivity analysis is performed to investigate the effects of increasing or decreasing these rates on the system reliability. Similarly, component importance is analysed to find out the importance of each component on the reliability of the overall system architecture.

3.1 Reliability

Reliability is the probability that a system performs its mission successfully for a given period of time. A system comprises of number of components and each component has two states: operating or failed. Component reliability is the probability that a component is operating successfully in a given period of time. System reliability depends upon component reliability of each component and the design of the system. System operates successfully if all the components operate successfully. However, even when a subset of components has failed, system may still operate successfully. Availability is similar to reliability and is defined as the probability that a system is operating successfully at a given time.

3.2 Reliability Modeling

There are many different methods of reliability modeling. This thesis uses the reliability block diagram (RBD) method. For this method, RBD are drawn for each system, where each block represents a component or a group of components. In RBD, components that are used together to perform a function are put in series whereas redundant components are put in parallel [58]. Next step is to formulate mathematical equations for reliability evaluation.

Evaluation procedure is presented in detail for each architecture. Comparative studies are performed in order to evaluate how a system reliability depends on the arrangement of components in architecture design and failure and repair rates of individual components.

Two models, repairable and non-repairable, are used to illustrate the effects of component repairs in reliability modeling. Repairable model with reasonable repair rates can significantly improve the reliability of a system. This thesis also investigates the other indices of reliability, namely MTTF and MTTFF. These indices are used to estimate the length of time it take for a new system or newly repaired system to fail. Mathematical expressions are derived for availability, MTTF, MTTFF, repair rates, and failure rates. Repair rates and failure rates for individual components are used to quantitatively evaluate each of the architecture in terms of these expressions. In addition, sensitivity analysis is carried out to investigate the effects of increasing/decreasing failure and repair rates on system reliability. Further, component importance is computed to illustrate how each component contributes to the overall reliability of the system. This will help to identify the critical components within the substation architecture, especially in light of improving the system reliability.

Some assumptions are made for simplicity of reliability modeling. First assumption is that components fail independently of each other. Second, each component has constant failure and repair rates. Estimated failure and repair rates for each component provided by the manufacturer are used for the analysis. For the components whose manufacturer-provided rates are unknown, hypothesized rates are used. It would be interesting to see how the cybersecurity related failures and repairs impact on the system reliability. Since the measurement depends on the structure of the RBD, it is important to draw the RBD correctly.

3.3 Ten Common Substation Communication Architectures

Commercial Information technologies such as Ethernet, TCP/IP, and Windows operating system are used for communication for both critical and non-critical infrastructure [59]. Although the interfacing of control equipment is made convenient by the use of such commercial products, due to the lack of security in such products isolation of the substation network (SN) with corporate network (CN) is essential. Firewall, router, and DMZ between networks are common ways how these two networks can be separated. Most common way of isolating a control network from industrial or corporate network is by using firewalls. However, effectiveness of firewall on its own in control environment is debatable. Therefore, substation networks have deployed various architectures beyond firewalls to isolate themselves from the corporate network. Ten such common architectures are investigated in this thesis [18, 59].

3.3.1 Dual-Homed Computers (DHC)

This architecture shown in Fig. 9 consists of installation of dual network interface cards (NICs) in computers that lie between CN and SN. DHC can send and receive packets from both networks, but does not allow the two networks to communicate directly, at least in theory. However, it allows minimal network separation. Network configuration can be adjusted so that DHC allows devices from one network to automatically forward packets

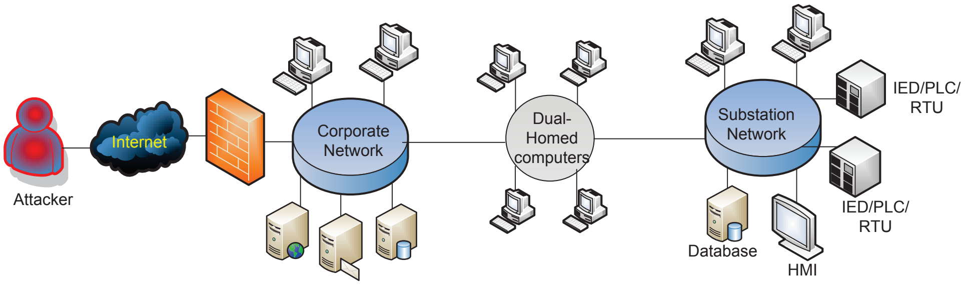


Figure 9: Dual-Homed Computers (Architecture 1)

to the other network. In such case, the main purpose of network isolation is defeated. DHCs are widely viewed as convenient targets by hackers.

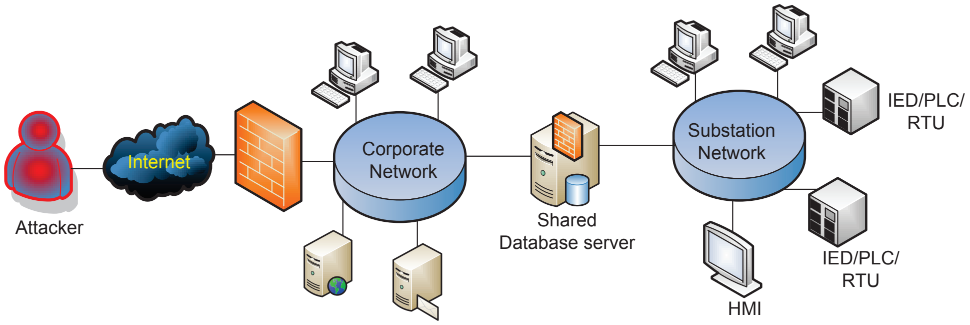


Figure 10: Dual-Homed Server (Architecture 2)

3.3.2 Dual-Homed Server (DHS)

This architecture as shown in Fig. 10 is similar to the DHC architecture, but in this case network of DHCs is replaced by a single server. Usually, a host-based firewall is installed in such server which will allow the traffic flow between two networks. Typically, a historian server can be dual-homed server since it needs to be accessed by both networks. Just as in DHC, DHS will not allow direct communication of traffic between two networks. Any communication has to go through the shared server. This architecture requires less efforts to manage and it is convenient to share common data between two networks. However, it has poor security against traffic that has to travel from CN to SN.

3.3.3 Two-Port Firewall (FW)

A simple two-port firewall between CN and SN can be a convenient solution for network segregation in some cases as shown in the architecture of Fig. 11. Most commercial firewalls can inspect all TCP packets and act as proxy for common internet-based protocols such as FTP and HTTP [59]. If managed well, such firewalls can be successfully deployed to thwart most external attacks on SN. However, certain data such as historian server data needs to be accessed by both CN and SN. So, the firewall must contain a rule to allow such data transfer. However, malicious packets appearing to be historian data can be forwarded to SN using the same firewall rule. Although this type of firewall in itself can be considered secure, communication requirements of CN and SN between each other require vulnerable

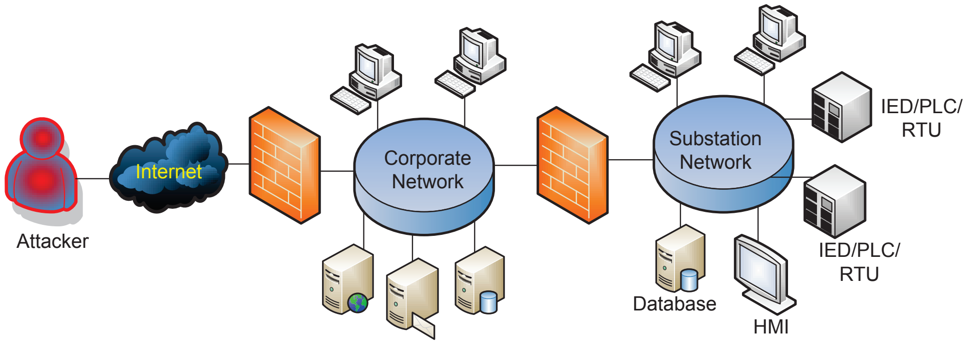


Figure 11: Two Firewalls (Architecture 3)

firewall rule-set that can be exploited by attackers.

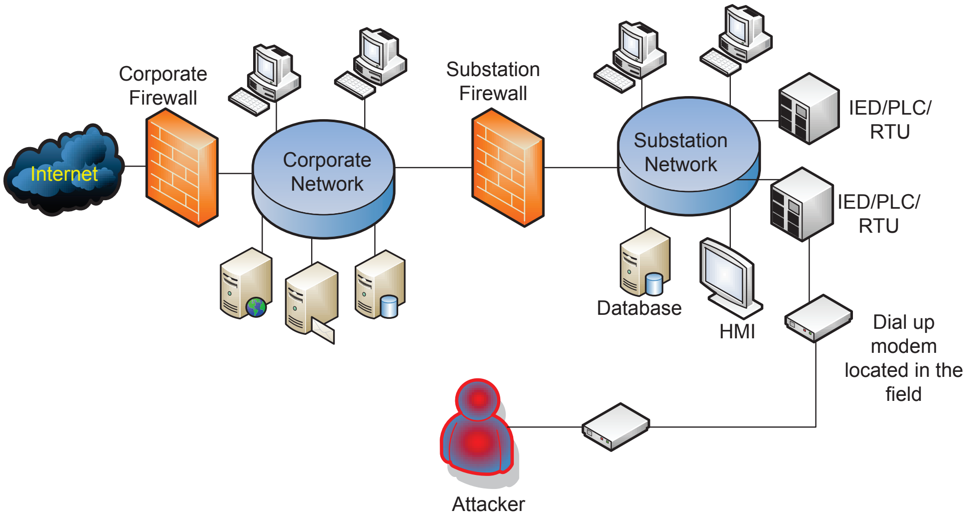


Figure 12: Dial-Up Access to RTUs (Architecture 4)

3.3.4 Dial-Up Access to RTUs

Dial-up modems (DUMs) are part of some SN and allow remote field devices and technicians to communicate directly with RTUs and other devices in the substation. These modems usually work as back-up pathways when primary communication fails. Attackers can exploit such communication by directly dialing the modems attached to the field devices. Attacker will dial every phone number looking for the modem. It is not very sophisticated to find these modems since most RTUs identify themselves. Successful connection to the modem creates an alternative path for the attacker to reach the SN. Such alternate path allows attacker to bypass firewalls and DMZs. However, the attacker must break the RTU authentication and know RTU protocol in order to control the RTU. The architecture as shown in Fig. 12 depicts the dial-up access to RTUs.

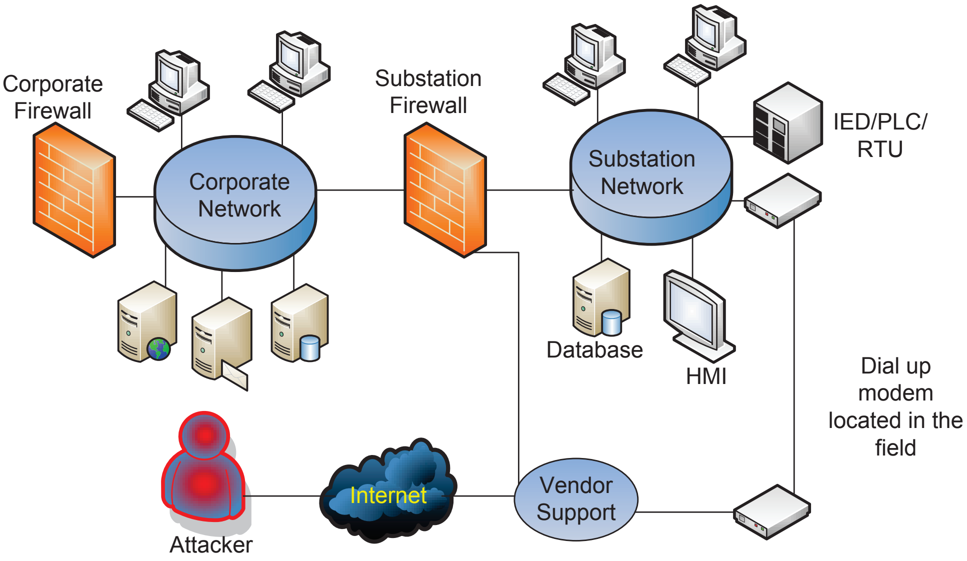


Figure 13: Vendor Support (Architecture 5)

3.3.5 Vendor Support

Many SNs have agreements with vendors for system upgrades, patching, and maintenance of the devices. A common means of vendors support is through a dial-up modem. This also creates an alternative path for the attacker. This architecture as shown in Fig. 13 accounts for such type of communication.

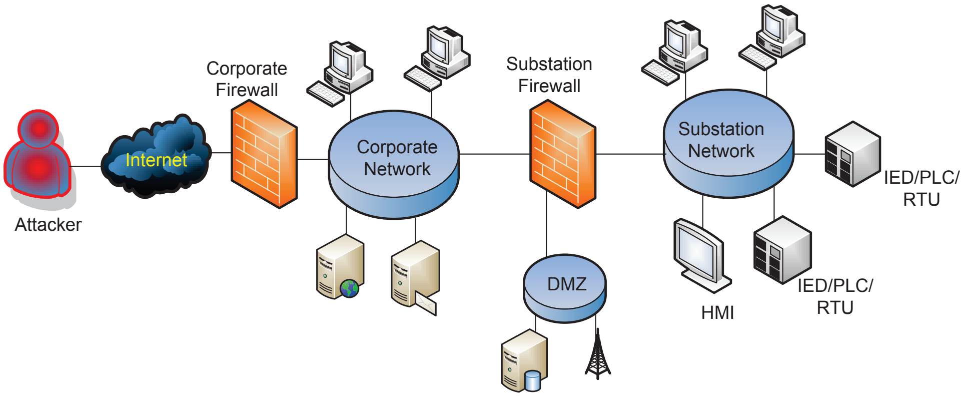


Figure 14: DMZ (Architecture 6)

3.3.6 Firewall with Demilitarized Zone (DMZ)

One or more DMZs between CN and SN can be a significant improvement in terms of security of SN. The architecture depicted in Fig. 14 shows such design. DMZ creates an intermediate network between the two networks. Firewall in DMZ requires three or more interfaces unlike two-port firewall. Each of CN and SN are connected to a separate interface. Third interface is connected to a shared network such as historian which sits inside the DMZ. No direct communication is possible between CN and SN as each communication initiated from these networks ends in the DMZ. Use of access control list will allow clear separation of the two networks. However, it is still possible for hackers to compromise a DMZ which would leave both CN and SN to be vulnerable.

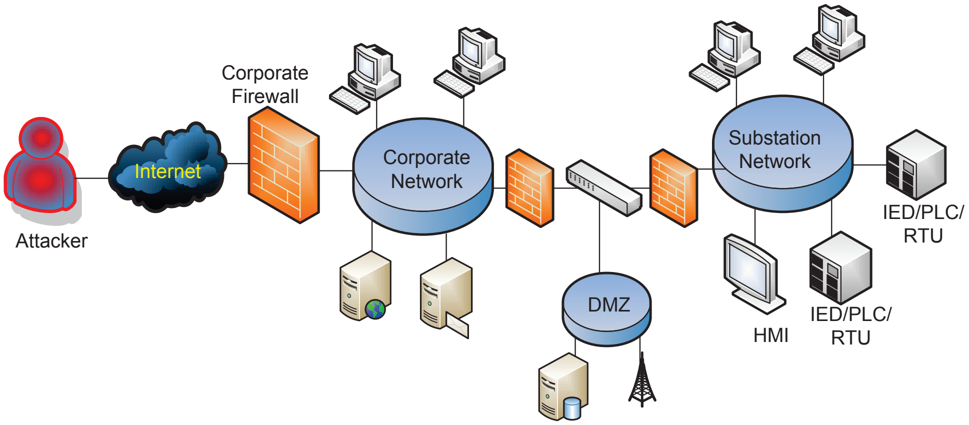


Figure 15: Paired Firewalls on Either Side of DMZ (Architecture 7)

3.3.7 A Firewall on Either Side of DMZ

DMZ can be made more secure by putting a firewall on each side of the DMZ. In this architecture as shown in Fig. 15, firewall on the CN side will prevent arbitrary packets from entering the DMZ. Similarly, firewall on the SN side will prohibit undesirable traffic from compromised server accessing the SN [59]. Using the two firewalls from two different manufacturers can further enhance security. Another advantage is that CN and SN can manage each firewall separately. It will however require increased cost.

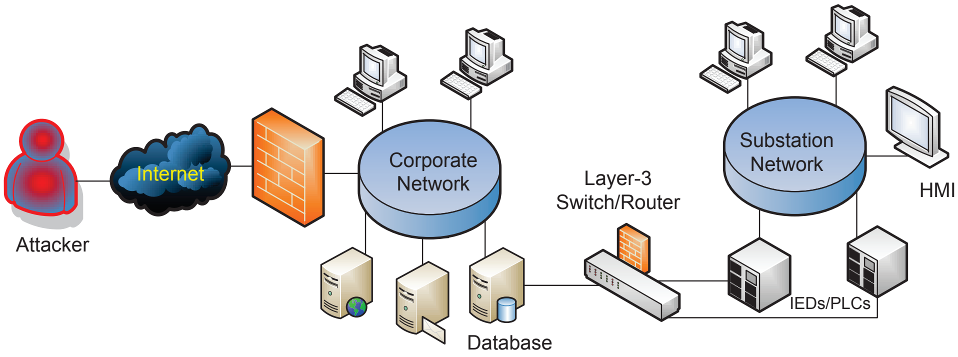


Figure 16: Packet-Filtering Router/Layer-3-Switch (Architecture 8)

3.3.8 Packet Filtering Ethernet Switch (ESW)/Router

This type of architecture as shown in Fig. 16 consists of a Ethernet switch usually a layer-3 or router between CN and SN. Usually, such switch is capable of basic filters to control traffic. Number of such switch/router work as packet filtering firewalls as well. These devices are capable of applying device to device rule-sets [59]. However, they cannot prevent attacks that use package fragmentation. So, they offer minimal protection against sophisticated attackers. This type of architecture is only secure if the CN is highly secure.

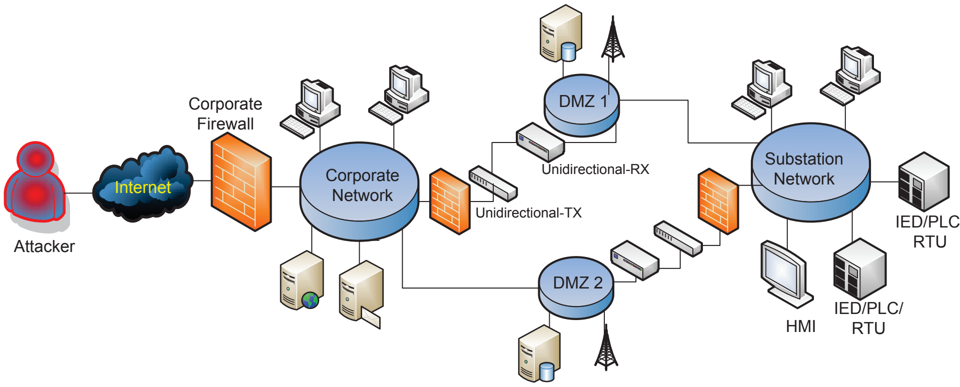


Figure 17: Unidirectional Gateways (Architecture 9)

3.3.9 Unidirectional Gateways

A more secure alternative is to use a combination of unidirectional gateways as a means to segregate CN and SN. The architecture as shown in Fig. 17 design utilizes two sets of unidirectional transmitters (TX) and two sets of unidirectional receivers (RX) creating two separate DMZs. The sending and receiving data from CN to SN uses separate DMZs. Each DMZ has data flowing in only one direction. The physical design of TX and RX prevents any back-flow of data. This type of architecture can be considered more secure compared to most other architectures.

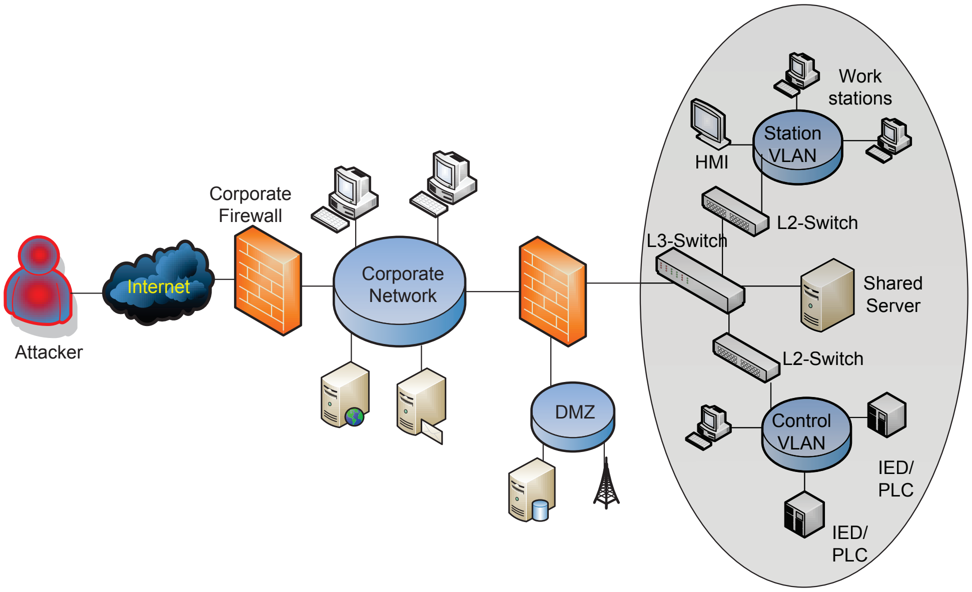


Figure 18: Substation VLANs (Architecture 10)

3.3.10 Firewall and Virtual LAN (VLAN)-Based SN

Previous architectures treat SN as a single network. However, SN can be separated into different VLANs where inter-area communication is not required. Simple layer-3 Ethernet switches can be used to control communication to such VLANs. On a same VLAN, Layer-2 switch can be used to control communication between devices. Architecture as shown in Fig. 18 contains three separate VLANs, one each for PLCs, historian server, and workstations. VLAN prevents unwanted traffic from flowing across the entire network. VLAN can also be useful against some internal attacks although it has a limited scope. If a DMZ and firewall are placed between CN and SN, this type of architecture can be very secure. Variations in design can be used depending upon the network.

3.4 Repairable System Model

RBD for architecture 1 is shown in Fig. 19. Here, the SN is a star topology which is same structure as architecture A from appendix. CN is linked to the SN by a network of n DHCs. For simplicity, n = 2 is used for rest of the paper. Mathematical analysis of general series and parallel structures of RBD are shown here [57]. System failure rate, repair rate, and probability of success are given by the equations below:

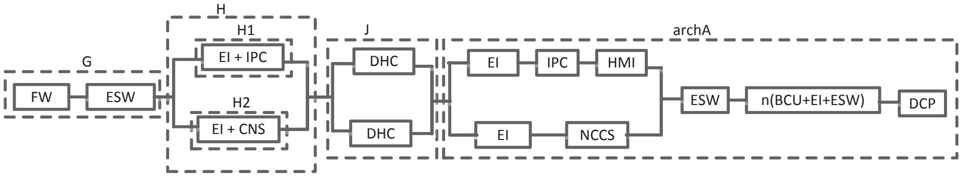


Figure 19: Reliability Block Diagram for Architecture 1

$$\lambda_{\text{sys}} = \lambda_1 + \lambda_2 \tag{1}$$

$$\mu_{\text{sys}} = \frac{\mu_1 \cdot \mu_2(\lambda_1 + \lambda_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2) - \mu_1 \cdot \mu_2} \tag{2}$$

$$P_{\text{s,sys}} = \frac{\mu_1 \cdot \mu_2}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)} \tag{3}$$

Similarly, for a parallel system, failure rate and repair rate are derived as follows:

$$\mu_{\text{sys}} = \mu_1 + \mu_2 \tag{4}$$

$$\lambda_{\text{sys}} = \frac{\lambda_1 \cdot \lambda_2(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2) - \lambda_1 \cdot \lambda_2} \tag{5}$$

MTTF for series combination of repairable systems can be calculated as follows:

$$\text{MTTF}_{\text{sys}} = \frac{1}{\lambda_{\text{sys}}} = \frac{1}{\lambda_1 + \lambda_2} \tag{6}$$

Similarly, MTTFF for a series system is calculated as follows:

$$\mathrm{MTTFF_{sys}} = \frac{1}{\lambda_{\mathrm{sys,MTTFF}}} = \frac{1}{\lambda_1 + \lambda_2} \tag{7}$$

For a parallel combination of repairable systems, MTTFF is calculated as shown by the equation below:

$$\mathrm{MTTFF_{sys}} = \frac{1}{\lambda_{\mathrm{sys,MTTFF}}} = \frac{(\lambda_1 + \lambda_2)(\lambda_1 + \mu_1 + \lambda_2 + \mu_2) + \mu_1 \cdot \mu_2}{\lambda_1 \cdot \lambda_2(\lambda_1 + \mu_1 + \lambda_2 + \mu_2)} \tag{8}$$

3.5 Non-Repairable System Model

This section shows the reliability calculations for non-repairable systems [57]. In a series combination, system reliability is the product of reliability of individual components as shown by the equation below:

$$R_{\mathrm{sys}} = P_{\mathrm{sys}} = P_1 \cdot P_2 \tag{9}$$

MTTF of a non-repairable system is expressed in terms of system reliability. For a parallel combination, system reliability is given as follows:

$$R_{\mathrm{sys}} = P_{\mathrm{sys}} = 1 - (1 - P_1)(1 - P_2) \tag{10}$$

Probability of success is expressed in terms of failure rate and time period as shown by equation below:

$$P = e^{-\lambda_{\mathrm{i}} \cdot \mathrm{t}} \tag{11}$$

The system reliability for a series combination is thus given by:

$$R_{\mathrm{sys}} = e^{-\lambda_1 \cdot \mathrm{t}} + e^{-\lambda_2 \cdot \mathrm{t}} \tag{12}$$

Now, MTTF of a is obtained by integrating reliability of the system from 0 to infinity as shown by the equation below:

$$MTTF = \int_0^\infty R_{\mathrm{sys}}(t)\,\mathrm{dt} \tag{13}$$

3.6 Repairable System Model

Using the above equations, mathematical expressions for repair rates, failure rates, MTTF, MTTFF, probability of success, availability, and reliability are are derived for architectures 1 to 10. Derivations of architecture 1 are show in this chapter. For the remaining architectures, derivations are listed in the appendix. Architecture A forms a part of architectures 1 through 9. The derivation for architecture A is also shown in appendix. Also listed in the appendix are the derivations for architecture A to D.

Following equations show the derivation of failure and repair rates for architecture 1. Architecture 1 is further divided into structures G, H, J, and architecture A; series combinations of these 4 structures form architecture 1. First, failure and repair rates for each of these structure are calculated separately. For structure G, failure and repair rates are expressed as follows:

$$\lambda_{\mathrm{G}} = \lambda_{\mathrm{FW}} + \lambda_{\mathrm{ESW}} \tag{14}$$

$$\mu_{\mathrm{G}} = \frac{\mu_{\mathrm{FW}} \cdot \mu_{\mathrm{ESW}}(\lambda_{\mathrm{FW}} + \lambda_{\mathrm{ESW}})}{(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}}) - \mu_{\mathrm{FW}} \cdot \mu_{\mathrm{ESW}}} \tag{15}$$

Structure H is further divided into structures H1 and H2. Failure and repair rates for H1 and H2 are expressed as follows:

$$\lambda_{\mathrm{H1}} = \lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}} \tag{16}$$

$$\mu_{\mathrm{H1}} = \frac{\mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}}(\lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}})}{(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{IPC}} + \mu_{\mathrm{IPC}}) - \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}}} \tag{17}$$

$$\lambda_{\mathrm{H2}} = \lambda_{\mathrm{EI}} + \lambda_{\mathrm{CNS}} \tag{18}$$

$$\mu_{\mathrm{H2}} = \frac{\mu_{\mathrm{EI}} \cdot \mu_{\mathrm{CNS}}(\lambda_{\mathrm{EI}} + \lambda_{\mathrm{CNS}})}{(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{CNS}} + \mu_{\mathrm{CNS}}) - \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{CNS}}} \tag{19}$$

Now, the failure and repair rates for H is expressed in terms of those rates for H1 and H2 as shown in the following equations:

$$\lambda_{\mathrm{H}} = \frac{\lambda_{\mathrm{H1}} \cdot \lambda_{\mathrm{H2}}(\mu_{\mathrm{H1}} + \mu_{\mathrm{H2}})}{(\lambda_{\mathrm{H1}} + \mu_{\mathrm{H1}})(\lambda_{\mathrm{H2}} + \mu_{\mathrm{H2}}) - \lambda_{\mathrm{H1}} \cdot \lambda_{\mathrm{H2}}} \tag{20}$$

$$\mu_{\mathrm{H}} = \mu_{\mathrm{H1}} + \mu_{\mathrm{H2}} \tag{21}$$

Similarly, failure and repair rates for J are derived:

$$\lambda_{\mathrm{J}} = \frac{2\lambda_{\mathrm{DHC}}^2 \cdot \mu_{\mathrm{DHC}}}{(\lambda_{\mathrm{DHC}} + \mu_{\mathrm{DHC}})^2 - \lambda_{\mathrm{DHC}}^2} \tag{22}$$

$$\mu_{\mathrm{J}} = 2\mu_{\mathrm{DHC}} \tag{23}$$

Now, the failure rate of architecture 1 is the sum of failure rates for G, H, J, and architecture A as shown by the equation below:

$$\lambda_{\mathrm{arch1}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H}} + \lambda_{\mathrm{J}} + \lambda_{\mathrm{archA}} \tag{24}$$

Similarly, repair rate of architecture 1 is expressed in terms of failure and repair rates of the 4 structures as shown by the equation below:

$$\mu_{\mathrm{arch1}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{J}} \cdot \mu_{\mathrm{archA}}(\lambda_{\mathrm{G}} + \lambda_{\mathrm{H}} + \lambda_{\mathrm{J}} + \lambda_{\mathrm{archA}})}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}})(\lambda_{\mathrm{J}} + \mu_{\mathrm{J}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}}) - \mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{J}} \cdot \mu_{\mathrm{archA}}} \tag{25}$$

3.6.1 MTTF

Now, the MTTF for architecture 1 is calculated as the reciprocal of the system failure rate as shown below:

$$\mathrm{MTTF}_{\mathrm{arch1}} = \frac{1}{\lambda_{\mathrm{arch1}}} \tag{26}$$

3.6.2 Probability of Success (P)

Probability of success is calculated using failure and repair rates of G, H, J, and arch 1 as shown by the equation below:

$$P_{\mathrm{s,arch1}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{J}} \cdot \mu_{\mathrm{archA}}}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}})(\lambda_{\mathrm{J}} + \mu_{\mathrm{J}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}})} \tag{27}$$

3.6.3 Availability (A)

Availability is the same as the probability of success as shown below:

$$A_{\mathrm{arch1}} = P_{\mathrm{s,arch1}} \tag{28}$$

3.6.4 MTTFF

MTTFF for repairable architecture 1 is calculated in the following steps. First, the failure rate for MTTFF is found for H and J. Failure rate for MTTFF of G is the same as that of MTTF. MTTFF failure rate for architecture A is calculated as shown in the appendix. System failure rate is the sum of the failure rates for these 4 structures. The following equations show these mathematical expressions:

$$\lambda_{\mathrm{H,MTTFF}} = \frac{\lambda_{\mathrm{H1}} \cdot \lambda_{\mathrm{H2}}(\lambda_{\mathrm{H1}} + \mu_{\mathrm{H1}} + \lambda_{\mathrm{H2}} + \mu_{\mathrm{H2}})}{(\lambda_{\mathrm{H1}} + \lambda_{\mathrm{H2}})(\lambda_{\mathrm{H1}} + \mu_{\mathrm{H1}} + \lambda_{\mathrm{H2}} + \mu_{\mathrm{H2}}) + \mu_{\mathrm{H1}} \cdot \mu_{\mathrm{H2}}} \tag{29}$$

$$\lambda_{\mathrm{J,MTTFF}} = \frac{2\lambda_{\mathrm{DHC}}^2(\lambda_{\mathrm{DHC}} + \mu_{\mathrm{DHC}})}{4\lambda_{\mathrm{DHC}}(\lambda_{\mathrm{DHC}} + \mu_{\mathrm{DHC}}) + \mu_{\mathrm{DHC}}^2} \tag{30}$$

$$\lambda_{\mathrm{arch1,MTTFF}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}} + \lambda_{\mathrm{J,MTTFF}} + \lambda_{\mathrm{archA,MTTFF}} \tag{31}$$

MTTFF is the reciprocal of the total failure rate.

$$\mathrm{MTTFF}_{\mathrm{arch1}} = \frac{1}{\lambda_{\mathrm{arch1,MTTFF}}} \tag{32}$$

3.7 Non-Repairable System Model

Reliability of non-repairable model of architecture 1 is found as shown by the following equations. Reliability for the structure G is calculated as follows:

$$P_{\mathrm{G}} = P_{\mathrm{FW}} \cdot P_{\mathrm{ESW}} \tag{33}$$

Similarly, reliability for H is calculated by the following equations:

$$
\begin{aligned}
P_{\mathrm{H1}} &= P_{\mathrm{EI}} \cdot P_{\mathrm{IPC}} && (34)\\
&= P_{\mathrm{EI}} \cdot P_{\mathrm{CNS}} && (35)\\
&= P_{\mathrm{H1}} + P_{\mathrm{H2}} - P_{\mathrm{H1}} \cdot P_{\mathrm{H2}} && (36)
\end{aligned}
$$

Next, reliability for J is expressed as follows:

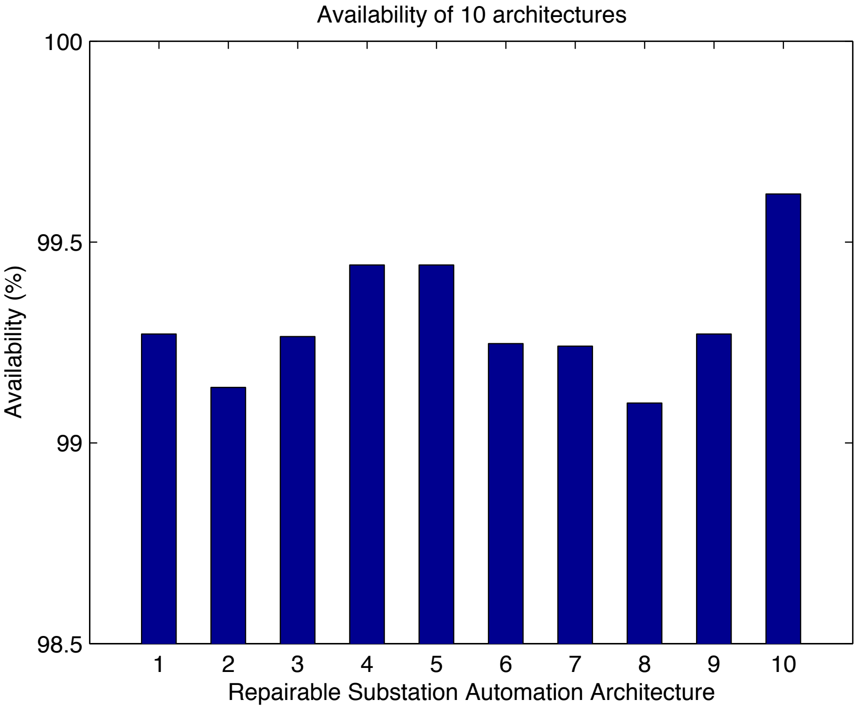


Figure 20: Availability of Repairable Architectures

$$P_{\mathrm{J}} = 2P_{\mathrm{DHC}} - P_{\mathrm{DHC}}^2 \tag{37}$$

Expression for architecture A is presented in the appendix. Using the expressions for these four structures, reliability of architecture 1 is calculated as the product of individual reliability as shown by the equation below:

$$R_{\mathrm{arch1}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{J}} \cdot P_{\mathrm{archA}} \tag{38}$$

3.8 Results

Availability of repairable systems for 10 architectures is presented in Fig. 20. In the figure, height of the bar represents availability. Comparisons can be made about which architecture is more available and which architecture is less available. The results show that availability of architecture 10 is the highest.

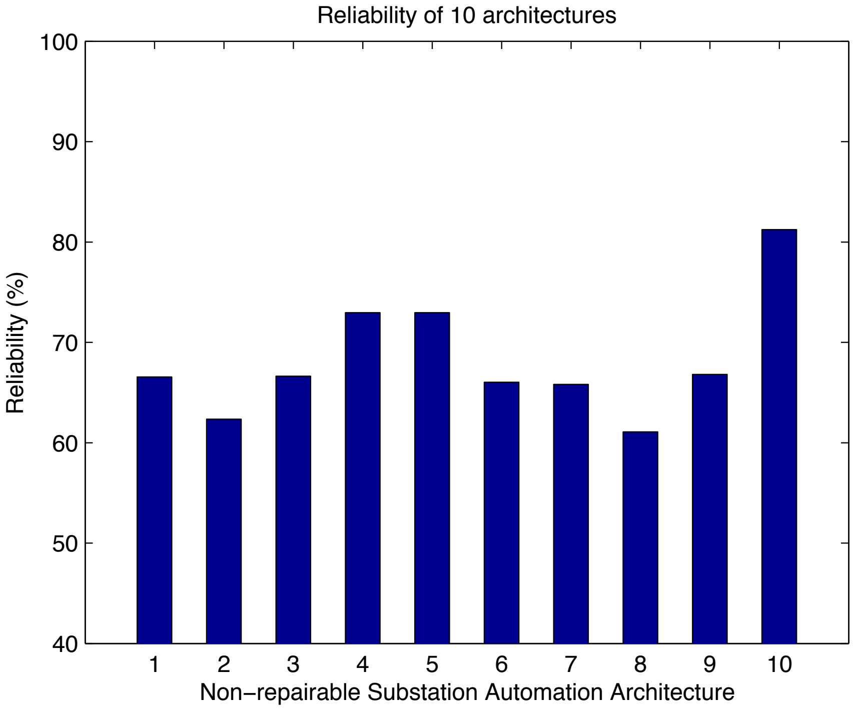


Figure 21: Reliability of Non-Repairable Architectures

Availability or reliability decreases significantly for non-repairable systems. Fig. 21 shows the reliability of 10 architectures for non-repairable system. Reliability ranking among the architectures is still in the same order as in repairable case. However, values are significantly lower for all of the architectures. This shows that repair plays an important role in making a system reliable.

Results for MTTF and MTTFF are shown in Fig. 22. As expected MTTF for repairable systems is higher than the non-repairable systems. This means that repairable systems operate for longer period of time before a failure occurs. MTTFF for non-repairable systems is not relevant because a failed component cannot be repaired for such systems and this quantity is not shown in the diagram. However, MTTFF for repairable system is shown which is similar to MTTF. The reason MTTF and MTTFF have similar values is because of the assumption of constant failure and repair rates. In practice, failure rates tend to increase with the age of the component which would give a different result.

Sensitivity here represents how the result changes when failure and repair rates change. variations of failure and repair rate in multiples of original rates are used to determine the sensitivity. Impact of such changes on MTTF for repairable system are determined for a number of combinations. Architecture 10 is used as the test case to demonstrate the findings. The results are shown in table 1. In the table, rows represent the multiples of repair rates and columns represent the multiple of failure rates.

Next, sensitivity of repair rates and failure rates are investigated separately. In the

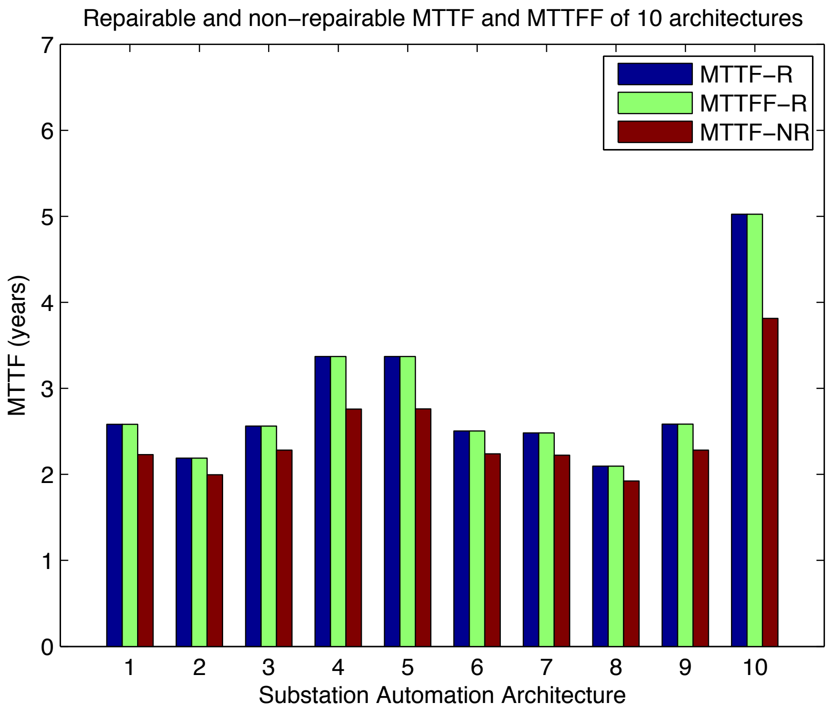


Figure 22: MTTF and MTTFF of Repairable and Non-Repairable Architectures

Table 1: Sensitivity of Repair and Failure Rates on MTTF of Architecture 10

	1×10^{-3}	1×10^{-2}	0.05	0.1	1	10
1×10^{-6}	2392.90	290.99	57.96	28.96	2.90	0.29
1×10^{-5}	4171.30	293.29	58.36	29.10	2.90	0.29
1×10^{-4}	4968.00	417.13	61.42	29.33	2.91	0.29
1×10^{-3}	5024.50	496.80	92.20	41.71	2.93	0.29
1×10^{-2}	5029.20	502.45	100.03	49.68	4.17	0.29
1×10^{-1}	5029.60	502.92	100.54	50.25	4.97	0.42
0.2	5029.60	502.94	100.57	50.27	5.00	0.46
0.5	5029.70	502.96	100.58	50.29	5.02	0.49
1	5029.70	502.96	100.59	50.29	5.02	0.50
2	5029.70	502.97	100.59	50.29	5.03	0.50
5	5029.70	502.97	100.59	50.30	5.03	0.50
10	5029.70	502.97	100.59	50.30	5.03	0.50
15	5029.70	502.97	100.59	50.30	5.03	0.50

first case, failure rates are kept constant and only the repair rates are varied by multiples. In the second case, repair rates are kept constant and failure rates are varied. In both cases, changes in repairable and non-repairable MTTF are studied. Fig. 23 and 24 show the result obtained for each scenario. Fig. 23 shows the sensitivity of component repair rates on repairable and non-repairable MTTF. Fig. 24 shows the sensitivity of component failure rates on repairable and non-repairable MTTF.

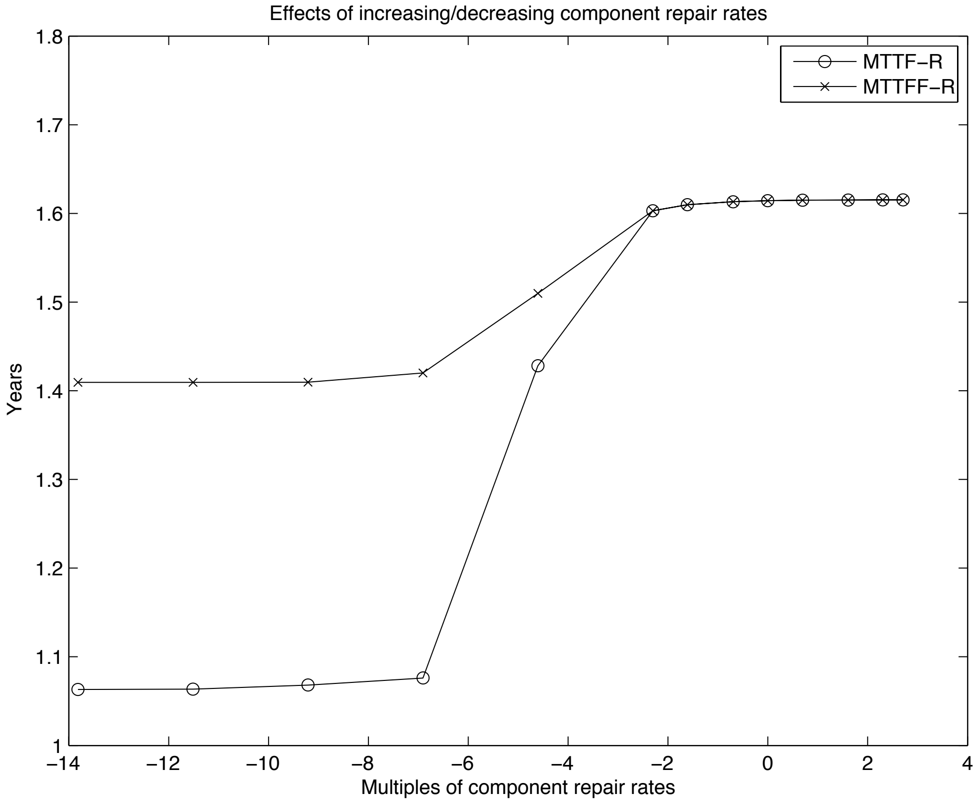


Figure 23: Sensitivity Analysis of Component Repair Rates on MTTF and MTTFF

4 Attack Tree Modeling for Substation Cybersecurity

In order to apply a defense mechanism to cybersecurity problem, enumeration of access points need to be exhaustively identified with an accurate assessment of the system vulnerability framework. An attack tree is a useful tool in modeling and analyzing the system vulnerability. Previous method show the use of attack graphs to demonstrate the path of a single attacker [60]. Howevever, in such models creating an attacker profile is necessary which will not be feasible for unknown attackers. In addition, such models are focused on a single attacker and multiple graphs are needed for multiple attackers. This chapter describes the attack tree method that is designed and analyzed for multiple unknown attacks on a substation network. The analysis is evaluated based on indicators for cost, technical proficiency of attackers, breach of trust, and noticeability. The proposed method can be applied to evaluate potential cyber-threats in a substation network environment to identify weaknesses for improvements.

4.1 Overview

Many remote unmanned substations have limited access by the vendors to constantly maintain the security posture of the system. The deficiency of substation security enhancement and protection can be exploited by the vulnerability in the network. Often,

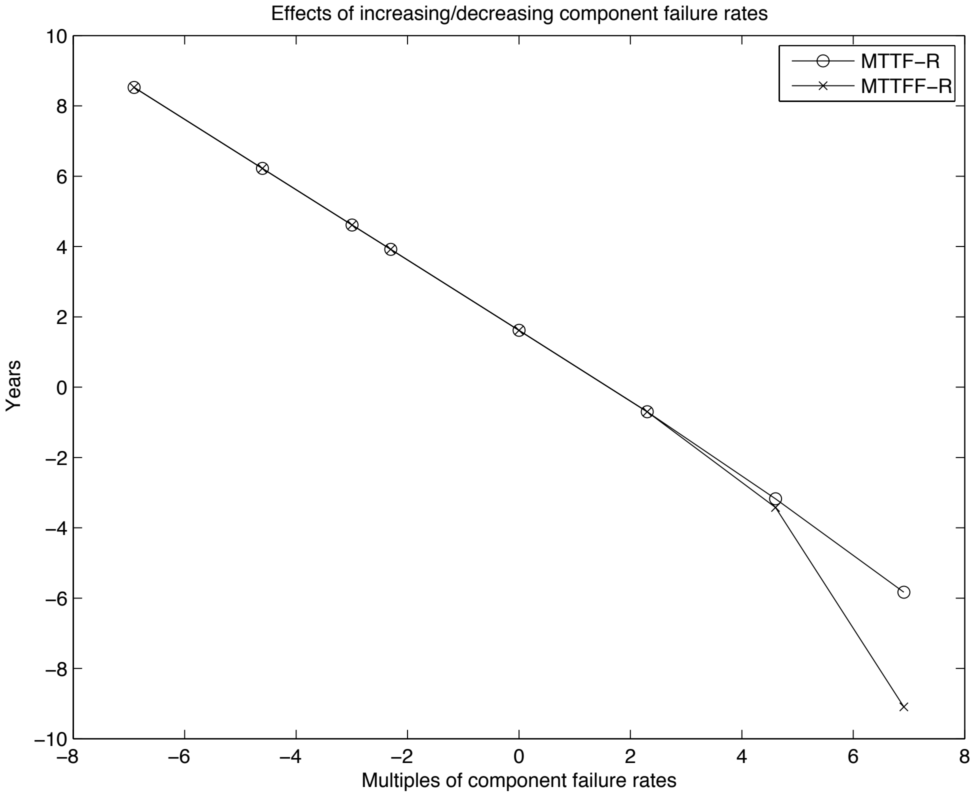


Figure 24: Sensitivity Analysis of Component Failure Rates on MTTF and MTTFF

these substation-level networks are connected to control center networks where critical access points may be penetrated by unauthorized users for malicious purpose. Substation facilities such as power transformers, switchgear, and microprocessor-based protection relays are considered critical infrastructure. The operations and monitoring of such facilities can be accessed through the user interface in the substation network. This can also be accessed by a cyber-intruder who has malicious intent to gain control over the network to plan for an attack.

Due to the complexity of the access points and vulnerability, a graphical approach is needed to systematically enumerate the plausible events for a substation network. A logic-based method using attack tree is applied to this problem. The past contributions by other researchers in security community emphasizes on high-level abstraction that can be modeled by generic components such as firewall and password protections and relationship between network topology [61]. Depending on the nature of modeling, this approach has been utilized for modeling the client-server communication by identifying the general vulnerabilities pertaining to this problem [62]. Also, enumeration of trojan horse detection has been researched using the attack tree [63]. Other graph-theoretic methods include using Petri net model to connect the cyber-component with the physical system for an integrated modeling [64].

Although attack tree method provides promising features to logically connect between access points and vulnerability; however, this requires ongoing effort to maintain the vulnerability knowledge rules in the database. This knowledge-based technique is subject to AND and OR rule sets of a substation to represent the network security protection. The subsystem of attack tree includes leaf nodes with defined indicator criteria that are connected by the parent node which can be an AND or OR gate. This qualitative modeling for each subsystem can be flexibly reconfigured with a unique attribution of indicators to a specific network vulnerability.

4.2 Fault Tree

Fault tree is similar to attack tree, but it lacks semantics and expressiveness of an attack tree [65]. Fault trees graphically represent the interactions of faults in a system. Just like attack trees, fault trees have leafs and nodes that are connected with the logic AND/OR gates moving up in the hierarchy. However, fault trees represent the fault or shortcomings in the system and does not account for the characteristics of the adversary. Instead, attack trees represent the capacity, motivation, experience, and goals of an adversary. It is important to look at system vulnerability in terms of adversary's perspective as well. In addition, fault trees lack the ability to capture the atomic details about the security threat [65]. Therefore, attack trees are designed to overcome the limitations of the fault tree and analyze system security from a different perspective [66].

4.3 Concept

Substation attack tree is represented by the vulnerability rule-set library to enumerate plausible events that may be exploited by attackers. This enumeration is modeled by leaf nodes combined with other rule sets of general information security to form the substation security adversary, which is the root node of the tree. Fig. 25 illustrates the qualitative modeling of the substation attack tree that consists of AND and OR logic gates.

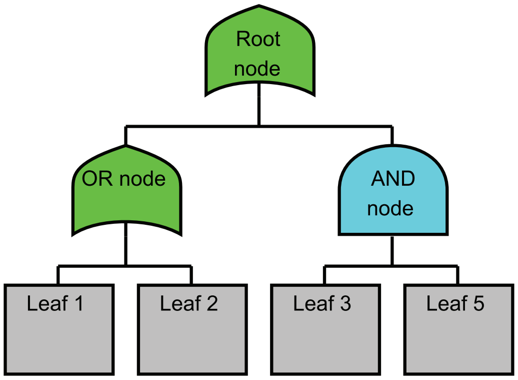


Figure 25: Attack Tree

In general, the leaf nodes (bottom of the tree nodes) do not have any child nodes which indicates the start of the scenario enumeration to the root node. The proposed model of hypothesized attack scenarios includes attackers' resource availability and their benefits that can be motivated by monetary rewards, technical ability of individual hackers, and time constraints. Most attackers' motive is to achieve financial goals, to access critical/useful information, and to gain their organization visibility.

Proposed method enumerates possible hypothesized scenarios of attackers' interest to compromise a substation network. The security analysts can utilize the qualitative modeling of the substation attack tree to identify the security bottleneck for future improvements. This chapter does not emphasize on the physical security. Instead, the attack tree enumeration for the substation networks is constructed based on the plausible attacks from outside of the network or within the network.

These are based on intrusion scenarios from the leaf nodes, *e.g.*, gaining access of the substation control network by cracking the administrative passwords either from corporate network or virtual private network (VPN). It all depends on the resources of attackers for which the option (s)he would be able to identify. Similarly, when a corporate network is compromised by the attacker, (s)he can identify other network access points to advance the attacks. For example, (s)he can send malwares, identify boundary protection rules for the gateways between other networks, or decipher the encryption for the data packets that traverse to other networks.

The attacker may decide utilizing fewer resources, which is not noticeable to network administrator. The attackers' footprints and plausible events can be translated into the scenarios for substation attack tree with indicators that attributed to attackers' level of strength and impact analysis. Formation of substation attack tree provide a ballpark number for system administrator to determine the worst case scenarios with possible improved countermeasures.

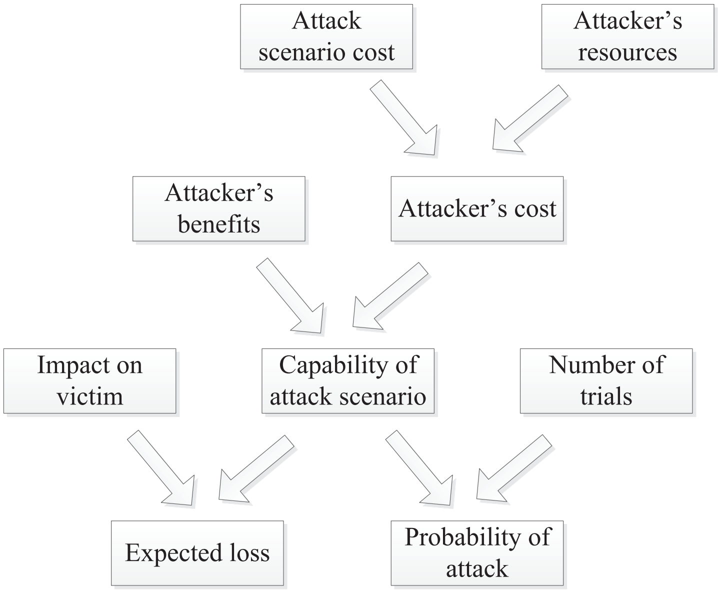


Figure 26: Vulnerability Analysis Flowchart

A flowchart is shown on Fig. 26 to explain the method of analyzing vulnerability using the attack tree. Probability of attack and expected loss are dependent on cost for each attack scenario, available resources, number of intrusion attempts, impact on substation operations, and benefits to attackers.

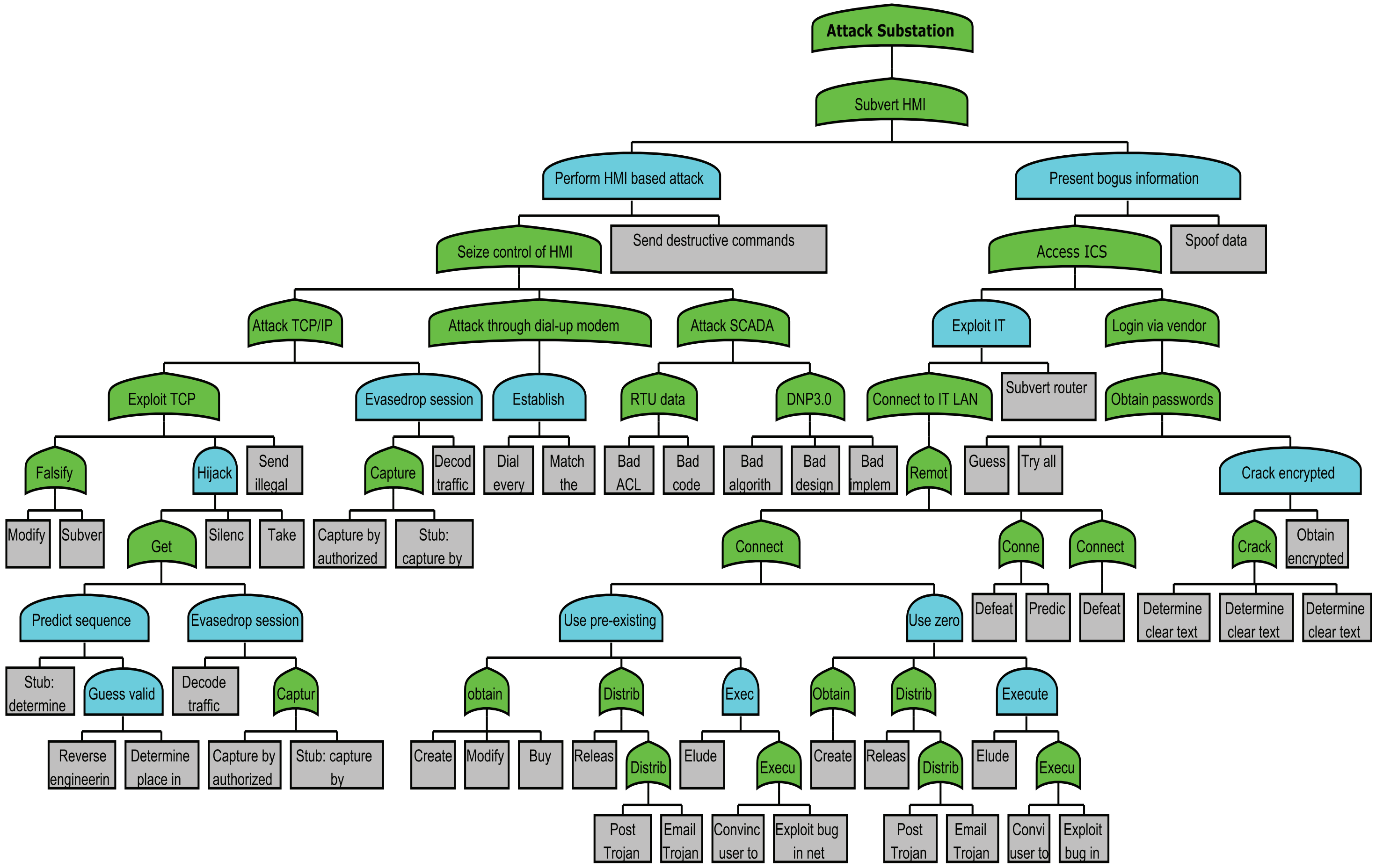


Figure 27: Attack Tree Model of Substation Network

4.4 Methodology

Fig. 27 is the attack tree model of a substation network shown in Fig. 1. Indicators are used to define the capability of the adversary, impacts on the defender's strategies, and the overall system of the adversary. These indicators are either boolean variables or variables represented by mathematical formula. For example, an attacker's willingness to spend certain amount of money on a particular attack could be linearly related to the amount of benefit to the attacker after the successful launching of an attack. How such attributes are given to the indicators depend upon estimates based upon expert opinion or statistical resources. Accuracy of such indicators depends upon the information available regarding the technology, previous attacks, and surveys. A novel attack which may not have occurred previously is still possible with the advancement in technology and the motivation of attacker. No matter how much information is gathered from previous occurrences of attacks, it is practically impossible to predict the occurrence of attacks. However, in absence of such methods, an estimate based on available knowledge can be a decent measure of vulnerability.

4.4.1 Capability of the Adversary

The indicators for the capability of adversary used in this thesis are breach of trust, cost of attack, defender error, noticeability, and technical ability. Breach of trust is a boolean variable and can be either true or false. It indicates if an insider's help is needed to launch a particular attack. Cost of attack is a continuous variable and it represents the total cost for a particular type of attack. The cost can range from few dollars to millions of dollars. An attack scenario that costs less financially is more likely to occur than a scenario with higher costs. Another indicator is a defender error which is also a true/false boolean indicator. An attacker may find loopholes in the network, software variants, or a misconfigured firewall to launch an attack. These scenarios are considered as errors of the defender and attackers will be looking towards capitalizing on such errors. Noticeability is also an important indicator of attacker's capability. An attack process that remains hidden from the defender is easy to carry out than an attack that will be noticeable. If the defender notices that the system is being breached, then the attacker's attempt will most likely be cut short. Final indicator of capability is technical ability which defines the level of expertise needed to carry out an attack scenario. Noticeability and technical ability are rated in a scale from 0 to 1, zero being the lowest and one being the highest. Such rating is relative and depends upon the expertise of the tree designer.

4.4.2 Attacker Impact vs. Defender Impact

There are two types of impacts from a particular attack: impact to the attacker and impact to the defender. Impact to the attacker is the benefit that the attacker gains after a successful attack or the punishment, fines, or jail-time that the attacker needs to pay/serve if the attacker is prosecuted. Benefit to the attacker can be financial benefit, technical benefits, destruction of equipment, and injuries to the public or any other factors that may motivate the attacker to launch an attack. However, attacker will be deterred by the amount of fine it needs to pay or the amount of jail-time it needs to serve if prosecuted. Similarly, there will be impacts on the defender which is different than the impact on the attacker. An attacker's loss may not be the same as defenders' benefit, so these two scenarios are considered separately. For example, an explosion of a transformer may cost millions of dollars to the utility, but the attacker may not gain as much.

4.4.3 Attack Tree Scenarios

There can be numerous possible ways for an adversary to compromise substation security to achieve specific goal. For example, an attacker may crack the password to a RTU server and change the current and voltage measurements or directly connect to the substation modem by bypassing the firewall rules. Enumeration of attack scenarios represent options available to attack's adversary. Graphically, these scenarios are sub-tree of the adversary. An attack tree represents the combination of such scenarios. Each scenario has some associated leaves and nodes and has associated attack costs and benefits. A simple attack scenario for the given attack tree is depicted in Fig. 28 and indicators for leaf nodes of the scenario are shown in Table I.

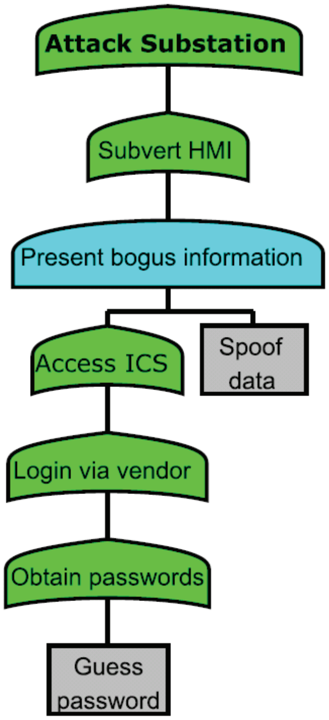
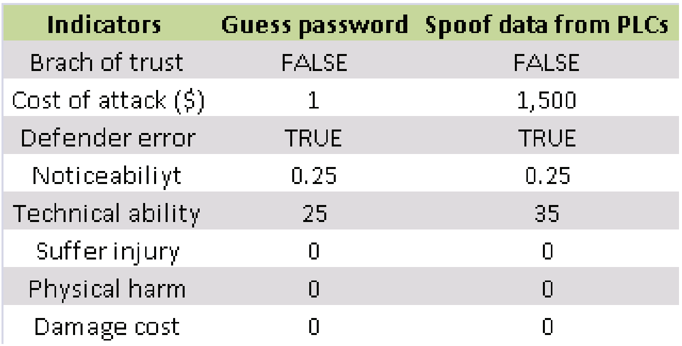


TABLE I
INDICATORS FOR LEAF NODES OF THE ATTACK SCENARIO



Indicators	Guess password	Spoof data from PLCs
Brach of trust	FALSE	FALSE
Cost of attack ($)	1	1,500
Defender error	TRUE	TRUE
Noticeabiliyt	0.25	0.25
Technical ability	25	35
Suffer injury	0	0
Physical harm	0	0
Damage cost	0	0

Figure 28: An Attack Scenario to Subvert HMI by Spoofing Data

4.5 Analysis and Results

Forty six different attack scenarios are identified for the attack tree depicted in Fig. 27. Each scenario has a cost and impact associated with it based on which the likelihood of the attack scenario taking place can be determined. The analysis includes the description of each scenario, which contains all of the leaves and nodes associated with the scenario. The majority of attack scenarios are based on following nodes:

4.5.1 Attack TCP/IP Vulnerabilities

- Falsify IP information
- Hijack session by obtaining sequence number
- Capture network by eavesdropping session

4.5.2 Access to Industrial Control System (ICS) Network

- Bypass firewall between ICS and substation network
- Connect through wireless
- Login via vendor
- Connect via VPN

4.5.3 Attack Upon SCADA System

- Attack RTU by exploiting access control list (ACL)
- Directly connect through dial-up modem
- Attack through DNP3 communication protocol

At the leaf level the following were identified as the root causes:

- Decode encryption
- Crack password
- Send malwares

Bad data are fed into the network or the destructive commands are sent once the communication barrier is breached. The vulnerability (V) of a particular attack scenario can be represented by the following matrix:

$$V = \begin{pmatrix} C \\ T \\ B \\ N \end{pmatrix}$$

Where C represents the cost indicator, T represents technical ability, B represents breach of trust, and N represents noticeability. Each leaf and node is represented in the same way as the attack scenario. Total number of indicators defines the size of the matrix. For an AND gate, for some of the variables such as cost of attack, the indicator values from the two or more leaves are added together at the node.

$$C = C_{1,2,\cdots,n} = C_1 + C_2 + \cdots + C_n$$

In case of technical ability, the maximum of the two or more vertices is taken.

$$T = T_{1,2,\cdots,n} = \max(T_1, T_2, \cdots, T_n)$$

Boolean OR is used to represent breach of trust. Since the value is 1 for "True" and 0 for "False," maximum of the two or more vertices is taken.

$$B = B_{1,2,\cdots,n} = \max(B_1, B_2, \cdots, B_n)$$

Noticeability is calculated by the following formula:

$$N = N_{1,2,\cdots,n} = 1 - [(1 - N_1)(1 - N_2) \cdots (1 - N_n)]$$

Thus, the vulnerability of an attack scenario based on attackers' resources is given by the following formula:

$$V = V_{1,2,\cdots,n}$$

$$\text{V} = \begin{pmatrix} C_1 + C_2 + \cdots + C_n \\ \max(T_1, T_2, \cdots, T_n) \\ \max(B_1, B_2, \cdots, B_n) \\ 1 - [(1 - N_1)(1 - N_2) \cdots (1 - N_n)] \end{pmatrix}$$

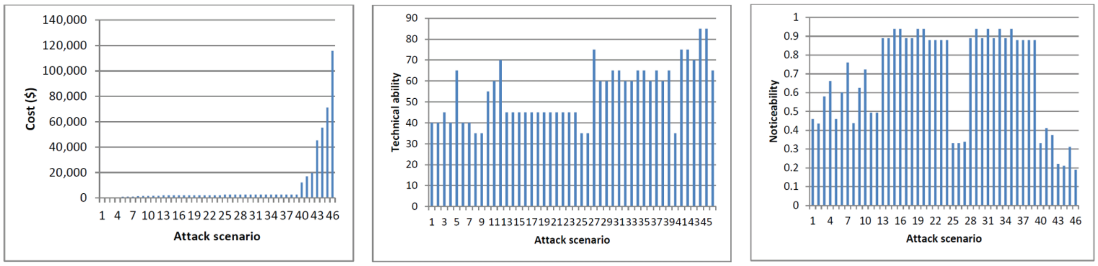


Figure 29: (a) Cost, (b) Technical Ability, and (c) Noticeability of Attack Scenarios

Fig. 29 show the resources needed to carry out each attack scenario. As shown in the graph, thirty nine scenarios cost less than $4,000 to carry out the attack. In other words, for someone who has $4,000 to spare, they have 39 different options to attack a substation network, given that they have the technical ability to carry out such attack. Goal of the utility that manages the substation should be to minimize the number of attack scenarios and increase the amount of resources required to carry out such attacks. The amount of resources required is directly related to the strengths of security measures applied. Similarly, increasing the noticeability and technical ability to higher values means that the possibility of an attack happening is even less likely.

Similar formula was used to represent impact indicators such as attacker benefit, attacker detriment, and victim impact. Attacker benefit and victim impact for the scenario was calculated using the sum of the vertices and attacker detriment was calculated as the maximum of vertices. Different formula was used for the nodes with the OR gate. Number of indicators and the formula can be changed to represent a specific network.

4.6 Work in Progress

The method presented in this chapter can be a starting point for future attack tree analysis of substation security. Readers may have some concerns about the method. Following are the efforts in answering such concerns:

1. Ability to quantify the values for technical ability, trust, and noticeability: It is true that these terms may not have absolute values or rather they vary from system to system. But there can be no denying that these terms play their role in cybersecurity.

2. Accuracy of assessment of the substation's actual risk: Cybersecurity risks arise from the weaknesses in the cyberinfrastructure and advancement of adversary capabilities. Although it is impossible to predict if certain type of attack will be carried out or not, it is not that intricate to say that the system has a defense mechanism for certain type of attack or the system is vulnerable to certain type of attack. We are interested in analyzing if the defense mechanism is adequate against various types of known attacks. For example, we can say that system is secure (or less vulnerable) against the password attack since the system has strong passwords.

3. Inclusion of new vulnerabilities: Sub-tree library is the essential part of the attack tree modeling. New sub-tree is created within the library if a new vulnerability is found. The tree structure is linked to the library and does not need much modification.

4. Novelty of attack trees to system network: The tree structure will be modified to represent the substation topology. Relays, actuators etc. that were missing in the previous tree structure will be added to represent a novel case for substation network.

5. Scalability of seemingly exhaustive approach: The attack tree example that was used in the paper was a single tree and does not contain any sub-trees. However, an attack tree can have many sub-trees contained within a tree. Main tree can be made to represent the topology of the substation network, while sub-trees are stored in the library and recalled only when necessary. Result will be: This will reduce the complexities in a tree structure as the main tree will be reduced in size. Single sub-tree will be sufficient to represent a single attack type. Library and the topology of the tree can be updated separately. Attacks can be filtered according to the security criteria.

5 Conclusion and Future Work

This thesis presents an overview on the present day substation architecture, cyber- vulnerabilities in substation architecture, and possible future improvements to enhance system security. This thesis also introduces unidirectional communication and difference between conventional bidirectional and unidirectional communication. In addition, different ways of attacks on a substation are listed. Enumeration of 10 common substation architectures is also presented in the paper. The major contribution of the paper is to present a reliability analysis of these 10 architectures. In addition, attack tree analysis method for vulnerability analysis of a substation architecture is presented. Attacker does not have the knowledge of a system operator. Attackers work based on their own knowledge base. So, knowing the power system from attacker's perspective is equally important. Attack tree analysis helps in enumerating vulnerabilities and identifying critical vulnerabilities from attackers perspective.

Quantifying cybersecurity is a major concern in the field of power system security. However, experts in the field have general understanding that confidentiality, integrity, and availability (CIA) are the three factors that contribute to the cybersecurity. Out of the three, availability and integrity are considered most important for power systems. This thesis presents quantitative analysis of reliability of various substation communication architectures. Reliability, availability, MTTF, and MTTFF are the basic quantities in reliability analysis. Failure rates and repair rates of individual components are taken as inputs in such analysis. Two models, repairable and non-repairable, are used to show the effects of repair on the system reliability. Effects of repair and failure rates of individual component and importance of each component in reliability of the system is analyzed. Based on the method, reliability analysis of any substation can be performed to find its vulnerability. Similarly, comparisons can be made between the architectures to find which architecture is more secure compared to other.

Attack tree analysis technique provides a new dimension of the assessment for cybersecurity problem in the substation-level network. Vulnerability of a network does not solely depend upon the historical events, but also depends upon the capability and motivation of the cyber-intruder. The proposed model focuses on cyber-related events from the attacker's perspective. The proposed attack tree formulation can be enhanced with specific network attribution in which its analysis can be used to predict the security flaws, impact assessment, and develop countermeasures for loosely mandated security measures, such as weak password policies, or default firewall rules. Effects of such practices can be alarming to system administrator to make improvements. There can be more complicated and intricate loopholes in security of a network, which can be studied with what-if countermeasure improvements using the base case of attack tree. Such measures will usually result in decreased number of possible attack scenarios and increased difficulty for attack scenarios.

Future work will be conducted by extensively researching the following items:

1. The relationship between failures and repairs impact on the system reliability.

2. Availability and accuracy of data is a major challenge in reliability studies. Trade-off studies comparing the monitoring costs vs. reliability enhancements and optimization for optimum monitoring points considering reliability and cost constraints can be done in the future to further this research.

3. Reliability analysis in this thesis mostly compares the existing architectures against each other. In the future, new architectures such as the combination of architectures 9 and 10, which has a VLAN as well as unidirectional gateways, can be studied. Such architecture can provide improved security.

4. Failure rates are based on two states, failed and working. A multi-state model can be used to include the transitional states where devices are partially operational or

are working with decreased efficiency.

5. Attack tree analysis presented in this thesis proposes a general representation of a typical substation network. In the future, this work can be extended to represent a specific substation configuration for accurate analysis. Future research includes network connectivity between substations, or substation and control center. This work establishes the fundamental attack tree library that can be enhanced to represent a more sophisticated network.

6. Instead of a tree structure, graphical method can be used to analyze the attack scenarios as well. Such structure can be useful to represent the actual propagation of attack.

6 References

[1] L. Pietre-Cambacedes, M. Tritschler, and G. Ericsson, "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs," *IEEE Trans. Power Del.*, vol. 26, no. 1, pp. 161 –172, jan. 2011.

[2] S. Hong, D.-Y. Shin, and M. Lee, "Evaluating security algorithms in the substation communication architecture," in *International Conference on Embedded Computing-Scalable Computing and Communications*, sep. 2009, pp. 314 –318.

[3] G. N. Ericsson, "Cybersecurity and power system communication- essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501 –1507, jul. 2010.

[4] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492 –1500, jul. 2010.

[5] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cybersecurity for smart grid communications," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 998 –1010, 2012.

[6] Z. Bo, B. Zhang, J. He, X. Dong, B. Caunce, and A. Klimek, "An integrated boundary protection scheme for power transmission line systems," in *International Power Engineering Conference*, dec. 2007, pp. 470 –475.

[7] H. Hengxu, Z. Baohui, and L. Zhilai, "The basic theory of boundary protection for EHV transmission lines," in *International Conference on Power System Technology*, vol. 4, 2002, pp. 2569 – 2574.

[8] L. Bensinger and D. Johnson, "Layering boundary protections: an experiment in information assurance," in *16th Annual Conference on Computer Security Applications*, dec. 2000, pp. 60 –66.

[9] M. Braendle, "Cybersecurity for power systems- a closer look at the drivers and how to best approach the new challenges," in *Annual Conference for Protective Relay Engineers*, apr. 2011, pp. 322 –327.

[10] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence, and M. Pozzuoli, "Secure SCADA network supporting NERC CIP," in *IEEE PES General Meeting*, jul. 2009, pp. 1 –8.

[11] R. Burt, "A small utility's perspective on CIP: version 4," in *IEEE PES Power Systems Conference and Exposition*, mar. 2011.

[12] M. Mertz, "NERC CIP compliance: We have identified our critical assets, now what?" in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, jul. 2008, pp. 1 –2.

[13] X. Yue, W. Chen, and Y. Wang, "The research of firewall technology in computer network security," in *Asia-Pacific Conference on Computational Intelligence and Industrial Applications*, vol. 2, nov. 2009, pp. 421 –424.

[14] R. Zalenski, "Firewall technologies," *IEEE Potentials*, vol. 21, no. 1, pp. 24 –29, feb./mar. 2002.

[15] M. Vandenwauver, J. Claessens, W. Moreau, C. Vaduva, and R. Maier, "Why enterprises need more than firewalls and intrusion detection systems," in *IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 1999, pp. 152 –157.

[16] M. H. Kang, I. S. Moskowitz, and S. Chincheck, "The pump: a decade of covert fun," *Annual Computer Security Applications Conference*, pp. 352–360, 2005.

[17] H. Okhravi and F. T. Sheldon, "Data diodes in support of trustworthy cyber infrastructure," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research.* NY, USA: ACM, 2010, pp. 1–4. [Online]. Available: http://doi.acm.org/10.1145/1852666.1852692

[18] US Cert. Control systems security program CSSP: overview of cyber vulnerabilities. [Online]. Available: http://www.us-cert.gov/control_systems/csvuls.html

[19] L. Pietre-Cambacedes and P. Sitbon, "An analysis of two new directions in control system perimeter security," in *Proceedings of the 3rd SCADA Security Scientific Symposium*, vol. 4, Miami, USA, jan. 2009, pp. 1–30.

[20] U.S. Government Accountability Office. (2004, Mar.) Technologies to secure federal systems. [Online]. Available: http://www.gao.gov/products/GAO-04-467

[21] H. Gharavi and B. Hu, "Multigate communication network for smart grid," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1028 –1045, jun. 2011.

[22] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1218 –1228, apr. 2011.

[23] Z. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 50 –55, sep.-oct. 2011.

[24] F. Caldeira, M. Castrucci, M. Aubigny, D. Macone, E. Monteiro, F. Rente, P. Simoes, and V. Suraci, "Secure mediation gateway architecture enabling the communication among critical infrastructures," in *Future Network and Mobile Summit*, jun. 2010, pp. 1 –8.

[25] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58 –66, jan.-feb. 2012.

[26] T. Sarma, A. Venugopal, and T. Srujana, “Evolving the system for remote control, configuration, and management,” in *IEEE Region 10 Conference*, nov. 2006, pp. 1 –4.

[27] B. Bennett and S. Transue, “Remote IP SATCOM monitoring and management,” in *IEEE Military Communications Conference*, nov. 2008, pp. 1 –5.

[28] M. Bastos and M. Machado, “Visual, real-time monitoring system for remote operation of electrical substations,” in *IEEE PES Transmission and Distribution Conference and Exposition: Latin America*, nov. 2010, pp. 417 –421.

[29] W. Zhong, Y. Zhang, and Y. Jiang, “The design of VPN security gateway in remote monitoring system of rheometer,” in *6th International Forum on Strategic Technology*, vol. 2, aug. 2011, pp. 1109 –1113.

[30] W. Zhang, Q. Yang, and Y. Geng, “A survey of anomaly detection methods in networks,” in *International Symposium on Computer Network and Multimedia Technology*, jan. 2009, pp. 1 –3.

[31] X. Wang, L. Pang, Q. Pei, and X. Li, “A scheme for fast network traffic anomaly detection,” in *International Conference on Computer Application and System Modeling*, vol. 1, oct. 2010, pp. 592 –596.

[32] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, “Network anomaly detection and classification via opportunistic sampling,” *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 6 –12, jan.-feb. 2009.

[33] W. Scheirer and M. C. Chuah, “Network intrusion detection with semantics-aware capability,” in *20th International Parallel and Distributed Processing Symposium*, apr. 2006.

[34] S. Chakraborty, S. Sarkar, and A. Ray, “Symbolic identification and anomaly detection in complex dynamical systems,” in *American Control Conference*, jun. 2008, pp. 2792 –2797.

[35] J. Fowler and Q. Du, “Anomaly detection and reconstruction from random projections,” *IEEE Trans. Image Process.*, vol. 21, no. 1, pp. 184 –195, jan. 2012.

[36] M. Thottan and C. Ji, “Anomaly detection in IP networks,” *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2191 – 2204, aug. 2003.

[37] K. Tan and R. Maxion, “Determining the operational limits of an anomaly-based intrusion detector,” *IEEE J. Sel. Areas Commun.*, vol. 21, no. 1, pp. 96 – 110, jan. 2003.

[38] C.-W. Ten, J. Hong, and C.-C. Liu, “Anomaly detection for cybersecurity of the substations,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865 –873, dec. 2011.

[39] Z. Xie, G. Manimaran, V. Vittal, A. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857 – 863, aug. 2002.

[40] A. Sologar and J. Moll, "Developing a comprehensive substation cyber security and data management solution," in *IEEE Power Engineering Society General Meeting*, 2006.

[41] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *IEEE Power and Energy Society General Meeting*, jul. 2010, pp. 1 –6.

[42] "IEEE standard for SCADA and automation systems," *IEEE Std C37.1-2007 (Revision of IEEE Std C37.1-1994)*, pp. 1 –143, may 2008.

[43] "IEEE trial-use standard for a cryptographic protocol for cyber security of substation serial links," *IEEE Std 1711-2010*, pp. 1 –49, feb. 2011.

[44] S. Hurd, R. Smith, and G. Leischner, "Tutorial: Security in electric utility control systems," in *61st Annual Conference for Protective Relay Engineers*, apr. 2008, pp. 304 –309.

[45] B. Gellman, "U.S. fears Al Qaeda cyber attacks," Jun. 2002. [Online]. Available: http://www.securityfocus.com/news/502

[46] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210 –224, jan. 2012.

[47] M. Qureshi, A. Raza, D. Kumar, S. S. Kim, U. S. Song, M. W. Park, H. S. Jang, and H. S. Yang, "A communication architecture for inter-substation communication," in *IEEE International Conference on Computer and Information Technology Workshops*, jul. 2008, pp. 577–582.

[48] J. M. O. Filho. (2008) Substation and control centers. [Online]. Available: http://www.pacw.org/fileadmin/doc/SummerIssue08/ons_summer08.pdf

[49] S. Savulescu, "Backup control center design and implementation criteria," in *IEEE Power and Energy Society General Meeting*, jul. 2011, pp. 1 –6.

[50] B. Shephard, M. Janssen, and M. Schubert, "Standardised communications in substations," in *IEEE Seventh International Conference on Developments in Power System Protection*, 2001, pp. 270 –274.

[51] X. Zhou, X. Ma, and H. Zhang, "Research on wireless OPC DA server for modbus," in *TMEE International Conference*, dec. 2011, pp. 625 –628.

[52] L. Cheng, "Study and application of DNP3.0 in SCADA system," in *International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT)*, vol. 9, aug. 2011, pp. 4563 –4566.

[53] T. Mander, F. Nabhani, L. Wang, and R. Cheung, “Data object based security for DNP3 over TCP/IP for increased utility commercial aspects security,” in *IEEE Power Engineering Society General Meeting*, jun. 2007, pp. 1 –8.

[54] J. Robinson, T. Saxton, A. Vojdani, D. Ambrose, G. Schimmel, R. Blaesing, and R. Larson, “Development of the intercontrol center communications protocol ICCP: power system control,” in *IEEE Power Industry Computer Application Conference*, may 1995, pp. 449 –455.

[55] C. Hoga and G. Wong, “IEC 61850: open communication in practice in substations,” in *IEEE PES Power Systems Conference and Exposition*, vol. 2, oct. 2004, pp. 618 – 623.

[56] C.-W. Ten, C.-C. Liu, and G. Manimaran, “Vulnerability assessment of cybersecurity for SCADA systems,” *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836 –1846, nov. 2008.

[57] H. Hajian-Hoseinabadi and M. E. H. Golshan, “Availability, reliability, and component importance evaluation of various repairable substation automation systems,” *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1358–1367, 2012.

[58] H. Hajian-Hoseinabadi, M. Hasanianfar, and M. E. H. Golshan, “Quantitative reliability assessment of various automated industrial substations and their impacts on distribution reliability,” *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1223–1233, 2012.

[59] Center for the Protection of National Infrastructure. Firewall deployment for SCADA and process control networks: Good practice guide. [Online]. Available: http://www.energy.gov

[60] J. Wing, *Scenario Graphs Applied to Network Security*, Y. Qian, J. Joshi, D. Tipper, and P. Krishnamurthy, Eds. Morgan Kaufmann Publishers, Elsevier, Inc., 2008.

[61] C.-W. Ten, C.-C. Liu, and M. Govindarasu, “Vulnerability assessment of cybersecurity for SCADA systems using attack trees,” in *IEEE Power Engineering Society General Meeting*, jun. 2007, pp. 1 –8.

[62] W. Li, J. Huang, and W. You, “Attack modeling for electric power information networks,” in *International Conference on Power System Technology (POWERCON)*, oct. 2010, pp. 1 –5.

[63] C. Jin, X.-Y. Wang, and H.-Y. Tan, “Dynamic attack tree and its applications on trojan horse detection,” in *Second International Conference on Multimedia and Information Technology (MMIT)*, vol. 1, apr. 2010, pp. 56 –59.

[64] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, “Petri net modeling of cyber-physical attacks on smart grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741 –749, dec. 2011.

[65] D. Mirembe and M. Muyeba, “Threat modeling revisited: Improving expressiveness of attack,” in *Second UKSIM European Symposium on Computer Modeling and Simulation*, sep. 2008, pp. 93 –98.

[66] P. Khand, “System level security modeling using attack trees,” in *International Conference on Computer, Control and Communication*, feb. 2009, pp. 1 –6.

7 Appendix

7.1 Repairable System Model

This section presents the mathematical model for calculation of equivalent failure and repair rates, MTTF, probability of success, availability, and MTTFF of repairable architectures A-D and 1-10. Architectures A-D and evaluation method are based on the model presented in [57, 58].

7.1.1 Architecture A

Following equations show the calculation of equivalent failure and repair rates for architecture A.

Failure rate of A1:

$$\lambda_{\mathrm{A1}} = \lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}} \tag{39}$$

Repair rate of A1:

$$\mu_{\mathrm{A1}} = \frac{\mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}} \cdot \mu_{\mathrm{HMI}}(\lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}})}{(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{IPC}} + \mu_{\mathrm{IPC}})(\lambda_{\mathrm{HMI}} + \mu_{\mathrm{HMI}}) - \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}} \cdot \mu_{\mathrm{HMI}}} \tag{40}$$

Failure rate of A2:

$$\lambda_{\mathrm{A2}} = \lambda_{\mathrm{EI}} + \lambda_{\mathrm{NCCS}} \tag{41}$$

Repair rate of A2:

$$\mu_{\mathrm{A2}} = \frac{\mu_{\mathrm{EI}} \cdot \mu_{\mathrm{NCCS}}(\lambda_{\mathrm{EI}} + \lambda_{\mathrm{NCCS}})}{(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{NCCS}} + \mu_{\mathrm{NCCS}}) - \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{NCCS}}} \tag{42}$$

Failure rate of A:

$$\lambda_{\mathrm{A}} = \frac{\lambda_{\mathrm{A1}} \cdot \lambda_{\mathrm{A2}}(\mu_{\mathrm{A1}} + \mu_{\mathrm{A2}})}{(\lambda_{\mathrm{A1}} + \mu_{\mathrm{A1}})(\lambda_{\mathrm{A2}} + \mu_{\mathrm{A2}}) - \lambda_{\mathrm{A1}} \cdot \lambda_{\mathrm{A2}}} \tag{43}$$

Repair rate of A:

$$\mu_{\mathrm{A}} = \mu_{\mathrm{A1}} + \mu_{\mathrm{A2}} \tag{44}$$

Failure rate of B:

$$\lambda_{\mathrm{B}} = 2(\lambda_{\mathrm{BCU}} + \lambda_{\mathrm{EI}} + \lambda_{\mathrm{ESW}}) \tag{45}$$

Repair rate of B:

$$\mu_{\mathrm{B}} = \frac{\mu_{\mathrm{BCU}}^2 \cdot \mu_{\mathrm{EI}}^2 \cdot \mu_{\mathrm{ESW}}^2(2\lambda_{\mathrm{BCU}} + 2\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}})}{(\lambda_{\mathrm{BCU}} + \mu_{\mathrm{BCU}})^2(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})^2(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})^2 - \mu_{\mathrm{BCU}}^2 \cdot \mu_{\mathrm{EI}}^2 \cdot \mu_{\mathrm{ESW}}^2} \tag{46}$$

Failure rate of architecture A:

$$\lambda_{\mathrm{archA}} = \lambda_{\mathrm{DCP}} + \lambda_{\mathrm{B}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A}} \tag{47}$$

Repair rate of architecture A:

$$\mu_{\mathrm{archA}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{B}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{A}}(\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{B}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A}})}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{B}} + \mu_{\mathrm{B}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}}) - \mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{B}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{A}}} \tag{48}$$

Mean Time To Failure (MTTF)

MTTF of architecture A is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{archA}} = \frac{1}{\lambda_{\mathrm{archA}}} \tag{49}$$

Probability of Success (P)

Probability of success of architecture A is calculated as follows:

$$P_{\mathrm{s,archA}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{B}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{A}}}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{B}} + \mu_{\mathrm{B}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}})} \tag{50}$$

Availability (A)

Availability of architecture A is calculated as follows:

$$A_{\mathrm{archA}} = P_{\mathrm{s,archA}} \tag{51}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture A.

Failure rate for MTTFF of architecture A:

$$\lambda_{\mathrm{A,MTTFF}} = \frac{\lambda_{\mathrm{A1}} \cdot \lambda_{\mathrm{A2}}(\lambda_{\mathrm{A1}} + \mu_{\mathrm{A1}} + \lambda_{\mathrm{A2}} + \mu_{\mathrm{A2}})}{(\lambda_{\mathrm{A1}} + \lambda_{\mathrm{A2}})(\lambda_{\mathrm{A1}} + \mu_{\mathrm{A1}} + \lambda_{\mathrm{A2}} + \mu_{\mathrm{A2}}) + \mu_{\mathrm{A1}} \cdot \mu_{\mathrm{A2}}} \tag{52}$$

MTTFF of architecture A:

$$\mathrm{MTTFF}_{\mathrm{archA}} = \frac{1}{\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{B}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A,MTTFF}}} \tag{53}$$

7.1.2 Architecture B

Following equations show the calculation of equivalent failure and repair rates for architecture B.

Failure rate of C1:

$$\lambda_{\mathrm{C1}} = \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}} \tag{54}$$

Repair rate of C1:

$$\mu_{\mathrm{C1}} = \frac{\mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}} \cdot \mu_{\mathrm{HMI}}(\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{EI}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}})}{(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{IPC}} + \mu_{\mathrm{IPC}})(\lambda_{\mathrm{HMI}} + \mu_{\mathrm{HMI}}) - \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{IPC}} \cdot \mu_{\mathrm{HMI}}} \tag{55}$$

Failure rate of C2:

$$\lambda_{\mathrm{C2}} = \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{EI}} + \lambda_{\mathrm{NCCS}} \tag{56}$$

Repair rate of C2:

$$\mu_{\mathrm{C2}} = \frac{\mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{NCCS}}(\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{EI}} + \lambda_{\mathrm{NCCS}})}{(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})(\lambda_{\mathrm{NCCS}} + \mu_{\mathrm{NCCS}}) - \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{EI}} \cdot \mu_{\mathrm{NCCS}}} \tag{57}$$

Failure rate of C:

$$\lambda_{\mathrm{C}} = \frac{\lambda_{\mathrm{C1}} \cdot \lambda_{\mathrm{C2}}(\mu_{\mathrm{C1}} + \mu_{\mathrm{C2}})}{(\lambda_{\mathrm{C1}} + \mu_{\mathrm{C1}})(\lambda_{\mathrm{C2}} + \mu_{\mathrm{C2}}) - \lambda_{\mathrm{C1}} \cdot \lambda_{\mathrm{C2}}} \tag{58}$$

Repair rate of C:

$$\mu_{\mathrm{C}} = \mu_{\mathrm{C1}} + \mu_{\mathrm{C2}} \tag{59}$$

Failure rate of D:

$$\lambda_{\mathrm{D}} = 2(\lambda_{\mathrm{BCU}} + \lambda_{\mathrm{EI}}) \tag{60}$$

Repair rate of D:

$$\mu_{\mathrm{D}} = \frac{\mu_{\mathrm{BCU}}^2 \cdot \mu_{\mathrm{EI}}^2(2\lambda_{\mathrm{BCU}} + 2\lambda_{\mathrm{EI}})}{(\lambda_{\mathrm{BCU}} + \mu_{\mathrm{BCU}})^2(\lambda_{\mathrm{EI}} + \mu_{\mathrm{EI}})^2 - \mu_{\mathrm{BCU}}^2 \cdot \mu_{\mathrm{EI}}^2} \tag{61}$$

Failure rate of architecture B:

$$\lambda_{\mathrm{archB}} = \lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{C}} \tag{62}$$

Repair rate of architecture B:

$$\mu_{\mathrm{archB}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{C}}(\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{C}})}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{C}} + \mu_{\mathrm{C}}) - \mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{C}}} \tag{63}$$

Mean Time To Failure (MTTF)

MTTF of architecture B is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{archB}} = \frac{1}{\lambda_{\mathrm{archB}}} \tag{64}$$

Probability of Success (P)

Probability of success of architecture B is calculated as follows:

$$P_{\mathrm{s,archB}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}} \cdot \mu_{\mathrm{C}}}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})(\lambda_{\mathrm{C}} + \mu_{\mathrm{C}})} \tag{65}$$

Availability (A)

Availability of architecture B is calculated as follows:

$$A_{\mathrm{archB}} = P_{\mathrm{s,archB}} \tag{66}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture B.

Failure rate for MTTFF of C:

$$\lambda_{\mathrm{C,MTTFF}} = \frac{\lambda_{\mathrm{C1}} \cdot \lambda_{\mathrm{C2}}(\lambda_{\mathrm{C1}} + \mu_{\mathrm{C1}} + \lambda_{\mathrm{C2}} + \mu_{\mathrm{C2}})}{(\lambda_{\mathrm{C1}} + \lambda_{\mathrm{C2}})(\lambda_{\mathrm{C1}} + \mu_{\mathrm{C1}} + \lambda_{\mathrm{C2}} + \mu_{\mathrm{C2}}) + \mu_{\mathrm{C1}} \cdot \mu_{\mathrm{C2}}} \tag{67}$$

MTTFF of architecture B:

$$\mathrm{MTTFF}_{\mathrm{archB}} = \frac{1}{\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{ESW}} + \lambda_{\mathrm{C,MTTFF}}} \tag{68}$$

7.1.3 Architecture C

Following equations show the calculation of equivalent failure and repair rates for architecture C.

Failure rate of architecture C:

$$\lambda_{\mathrm{archC}} = \lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A}} \tag{69}$$

Repair rate of architecture C:

$$\mu_{\mathrm{archC}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}}^2 \cdot \mu_{\mathrm{A}}(\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A}})}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})^2(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}}) - \mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}}^2 \cdot \mu_{\mathrm{A}}} \tag{70}$$

Mean Time To Failure (MTTF)

MTTF of architecture C is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{archC}} = \frac{1}{\lambda_{\mathrm{archC}}} \tag{71}$$

Probability of Success (P)

Probability of success of architecture C is calculated as follows:

$$P_{\mathrm{s,archC}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{ESW}}^2 \cdot \mu_{\mathrm{A}}}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})^2(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}})} \tag{72}$$

Availability (A)

Availability of architecture C is calculated as follows:

$$A_{\mathrm{archC}} = P_{\mathrm{s,archC}} \tag{73}$$

Mean Time To First Failure (MTTFF)

MTTFF of architecture C is calculated as follows:

$$\mathrm{MTTFF}_{\mathrm{archC}} = \frac{1}{\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{A,MTTFF}}} \tag{74}$$

7.1.4 Architecture D

Following equations show the calculation of equivalent failure and repair rates for architecture D.

Failure rate of F1:

$$\lambda_{\mathrm{F1}} = 2\lambda_{\mathrm{ESW}} \tag{75}$$

Repair rate of F1:

$$\mu_{\mathrm{F1}} = \frac{2\mu_{\mathrm{ESW}}^2 \cdot \lambda_{\mathrm{ESW}}}{(\lambda_{\mathrm{ESW}} + \mu_{\mathrm{ESW}})^2 - \mu_{\mathrm{ESW}}^2} \tag{76}$$

Failure rate of F:

$$\lambda_{\mathrm{F}} = \frac{2\lambda_{\mathrm{F1}}^2 \cdot \mu_{\mathrm{F1}}}{(\lambda_{\mathrm{F1}} + \mu_{\mathrm{F1}})^2 - \lambda_{\mathrm{F1}}^2} \tag{77}$$

Repair rate of F:

$$\mu_{\mathrm{F}} = 2\mu_{\mathrm{F1}} \tag{78}$$

Failure rate of architecture D:

$$\lambda_{\mathrm{archD}} = \lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{F}} + \lambda_{\mathrm{A}} \tag{79}$$

Repair rate of architecture D:

$$\mu_{\mathrm{archD}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{F}} \cdot \mu_{\mathrm{A}}(\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{F}} + \lambda_{\mathrm{A}})}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{F}} + \mu_{\mathrm{F}})(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}}) - \mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{F}} \cdot \mu_{\mathrm{A}}} \tag{80}$$

Mean Time To Failure (MTTF)

MTTF of architecture D is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{archD}} = \frac{1}{\lambda_{\mathrm{archD}}} \tag{81}$$

Probability of Success (P)

Probability of success of success of architecture D is calculated as follows:

$$P_{\mathrm{s,archD}} = \frac{\mu_{\mathrm{DCP}} \cdot \mu_{\mathrm{D}} \cdot \mu_{\mathrm{F}} \cdot \mu_{\mathrm{A}}}{(\lambda_{\mathrm{DCP}} + \mu_{\mathrm{DCP}})(\lambda_{\mathrm{D}} + \mu_{\mathrm{D}})(\lambda_{\mathrm{F}} + \mu_{\mathrm{F}})(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}})} \tag{82}$$

Availability (A)

Availability of architecture D is calculated as follows:

$$A_{\mathrm{archD}} = P_{\mathrm{s,archD}} \tag{83}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture D.

Failure rate for MTTFF of F:

$$\lambda_{\mathrm{F,MTTFF}} = \frac{2\lambda_{\mathrm{F1}}^2(\lambda_{\mathrm{F1}} + \mu_{\mathrm{F1}})}{4\lambda_{\mathrm{F1}}(\lambda_{\mathrm{F1}} + \mu_{\mathrm{F1}}) + \mu_{\mathrm{F1}}^2} \tag{84}$$

MTTFF of architecture D:

$$\mathrm{MTTFF}_{\mathrm{archD}} = \frac{1}{\lambda_{\mathrm{DCP}} + \lambda_{\mathrm{D}} + \lambda_{\mathrm{F,MTTFF}} + \lambda_{\mathrm{A,MTTFF}}} \tag{85}$$

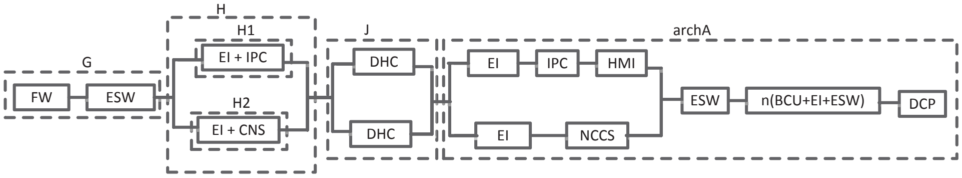


Figure 30: Reliability Block Diagram for Architecture 1

7.1.5 Architecture 1

Following equations show the calculation of equivalent failure and repair rates for architecture 1.

Failure rate of G:

$$\lambda_{\text{G}} = \lambda_{\text{FW}} + \lambda_{\text{ESW}} \tag{86}$$

Repair rate of G:

$$\mu_{\text{G}} = \frac{\mu_{\text{FW}} \cdot \mu_{\text{ESW}}(\lambda_{\text{FW}} + \lambda_{\text{ESW}})}{(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{ESW}} + \mu_{\text{ESW}}) - \mu_{\text{FW}} \cdot \mu_{\text{ESW}}} \tag{87}$$

Failure rate of H1:

$$\lambda_{\text{H1}} = \lambda_{\text{EI}} + \lambda_{\text{IPC}} \tag{88}$$

Repair rate of H1:

$$\mu_{\text{H1}} = \frac{\mu_{\text{EI}} \cdot \mu_{\text{IPC}}(\lambda_{\text{EI}} + \lambda_{\text{IPC}})}{(\lambda_{\text{EI}} + \mu_{\text{EI}})(\lambda_{\text{IPC}} + \mu_{\text{IPC}}) - \mu_{\text{EI}} \cdot \mu_{\text{IPC}}} \tag{89}$$

Failure rate of H2:

$$\lambda_{\text{H2}} = \lambda_{\text{EI}} + \lambda_{\text{CNS}} \tag{90}$$

Repair rate of H2:

$$\mu_{\text{H2}} = \frac{\mu_{\text{EI}} \cdot \mu_{\text{CNS}}(\lambda_{\text{EI}} + \lambda_{\text{CNS}})}{(\lambda_{\text{EI}} + \mu_{\text{EI}})(\lambda_{\text{CNS}} + \mu_{\text{CNS}}) - \mu_{\text{EI}} \cdot \mu_{\text{CNS}}} \tag{91}$$

Failure rate of H:

$$\lambda_{\text{H}} = \frac{\lambda_{\text{H1}} \cdot \lambda_{\text{H2}}(\mu_{\text{H1}} + \mu_{\text{H2}})}{(\lambda_{\text{H1}} + \mu_{\text{H1}})(\lambda_{\text{H2}} + \mu_{\text{H2}}) - \lambda_{\text{H1}} \cdot \lambda_{\text{H2}}} \tag{92}$$

Repair rate of H:

$$\mu_{\text{H}} = \mu_{\text{H1}} + \mu_{\text{H2}} \tag{93}$$

Failure rate of J:

$$\lambda_{\text{J}} = \frac{2\lambda_{\text{DHC}}^2 \cdot \mu_{\text{DHC}}}{(\lambda_{\text{DHC}} + \mu_{\text{DHC}})^2 - \lambda_{\text{DHC}}^2} \tag{94}$$

Repair rate of J:

$$\mu_{\text{J}} = 2\mu_{\text{DHC}} \tag{95}$$

Failure rate of architecture 1:

$$\lambda_{\text{arch1}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{J}} + \lambda_{\text{archA}} \tag{96}$$

Repair rate of architecture 1:

$$\mu_{\text{arch1}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{J}} \cdot \mu_{\text{archA}}(\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{J}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{J}} + \mu_{\text{J}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{J}} \cdot \mu_{\text{archA}}} \tag{97}$$

Mean Time to Failure (MTTF)

MTTF of architecture 5 is calculated as follows:

$$\text{MTTF}_{\text{arch1}} = \frac{1}{\lambda_{\text{arch1}}} \tag{98}$$

Probability of Success (P)

Probability of success of architecture 5 is calculated as follows:

$$P_{\text{s,arch1}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{J}} \cdot \mu_{\text{archA}}}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{J}} + \mu_{\text{J}})(\lambda_{\text{archA}} + \mu_{\text{archA}})} \tag{99}$$

Availability (A)

Availability of architecture 5 is calculated as follows:

$$A_{\text{arch1}} = P_{\text{s,arch1}} \tag{100}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 5.

Failure rate for MTTFF of H:

$$\lambda_{\text{H,MTTFF}} = \frac{\lambda_{\text{H1}} \cdot \lambda_{\text{H2}}(\lambda_{\text{H1}} + \mu_{\text{H1}} + \lambda_{\text{H2}} + \mu_{\text{H2}})}{(\lambda_{\text{H1}} + \lambda_{\text{H2}})(\lambda_{\text{H1}} + \mu_{\text{H1}} + \lambda_{\text{H2}} + \mu_{\text{H2}}) + \mu_{\text{H1}} \cdot \mu_{\text{H2}}} \tag{101}$$

Failure rate for MTTFF of J:

$$\lambda_{\text{J,MTTFF}} = \frac{2\lambda_{\text{DHC}}^2(\lambda_{\text{DHC}} + \mu_{\text{DHC}})}{4\lambda_{\text{DHC}}(\lambda_{\text{DHC}} + \mu_{\text{DHC}}) + \mu_{\text{DHC}}^2} \tag{102}$$

Failure rate for MTTFF of architecture 1:

$$\lambda_{\text{arch1,MTTFF}} = \lambda_{\text{G}} + \lambda_{\text{H,MTTFF}} + \lambda_{\text{J,MTTFF}} + \lambda_{\text{archA,MTTFF}} \tag{103}$$

MTTFF of architecture 1:

$$\text{MTTFF}_{\text{arch1}} = \frac{1}{\lambda_{\text{arch1,MTTFF}}} \tag{104}$$

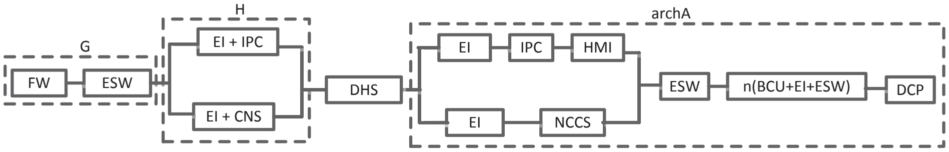


Figure 31: Reliability Block Diagram for Architecture 2

7.1.6 Architecture 2

Following equations show the calculation of equivalent failure and repair rates for architecture 2.

Failure rate of architecture 2:

$$\lambda_{\text{arch2}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{DHS}} + \lambda_{\text{archA}} \tag{105}$$

Repair rate of architecture 2:

$$\mu_{\text{arch2}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{DHS}} \cdot \mu_{\text{archA}}(\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{DHS}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{DHS}} + \mu_{\text{DHS}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{DHS}} \cdot \mu_{\text{archA}}} \tag{106}$$

Mean Time To Failure (MTTF)

MTTF of architecture 2 is calculated as follows:

$$\text{MTTF}_{\text{arch2}} = \frac{1}{\lambda_{\text{arch2}}} \tag{107}$$

Probability of Success (P)

Probability of success of architecture 2 is calculated as follows:

$$P_{\text{s,arch2}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{DHS}} \cdot \mu_{\text{archA}}}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{DHS}} + \mu_{\text{DHS}})(\lambda_{\text{archA}} + \mu_{\text{archA}})} \tag{108}$$

Availability (A)

Availability of architecture 2 is calculated as follows:

$$A_{\text{arch2}} = P_{\text{s,arch2}} \tag{109}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 2.

Failure rate for MTTFF of architecture 2:

$$\lambda_{\text{arch2,MTTFF}} = \lambda_{\text{G}} + \lambda_{\text{H,MTTFF}} + \lambda_{\text{DHS}} + \lambda_{\text{archA,MTTFF}} \tag{110}$$

MTTFF of architecture 2:

$$\text{MTTFF}_{\text{arch2}} = \frac{1}{\lambda_{\text{arch2,MTTFF}}} \tag{111}$$

7.1.7 Architecture 3

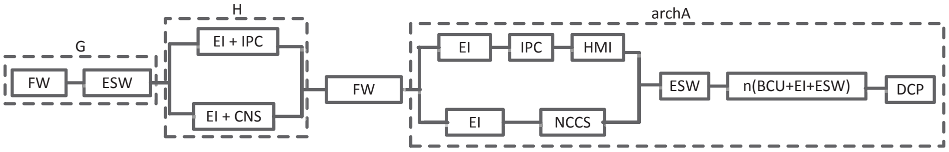


Figure 32: Reliability Block Diagram for Architecture 3

Following equations show the calculation of equivalent failure and repair rates for architecture 3.

Failure rate of architecture 3:

$$\lambda_{\text{arch3}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{FW}} + \lambda_{\text{archA}} \tag{112}$$

Repair rate of architecture 3:

$$\mu_{\text{arch3}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{FW}} \cdot \mu_{\text{archA}}(\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{FW}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{FW}} \cdot \mu_{\text{archA}}} \tag{113}$$

Mean Time To Failure (MTTF)

MTTF of architecture 3 is calculated as follows:

$$\text{MTTF}_{\text{arch3}} = \frac{1}{\lambda_{\text{arch3}}} \tag{114}$$

Probability of Success (P)

Probability of success of architecture 3 is calculated as follows:

$$P_{\text{s,arch3}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{FW}} \cdot \mu_{\text{archA}}}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{archA}} + \mu_{\text{archA}})} \tag{115}$$

Availability (A)

Availability of architecture 3 is calculated as follows:

$$A_{\text{arch3}} = P_{\text{s,arch3}} \tag{116}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 3.

Failure rate for MTTFF of architecture 3:

$$\lambda_{\text{arch3,MTTFF}} = \lambda_{\text{G}} + \lambda_{\text{H,MTTFF}} + \lambda_{\text{FW}} + \lambda_{\text{archA,MTTFF}} \tag{117}$$

MTTFF of architecture 3:

$$\text{MTTFF}_{\text{arch3}} = \frac{1}{\lambda_{\text{arch3,MTTFF}}} \tag{118}$$

7.1.8 Architecture 4

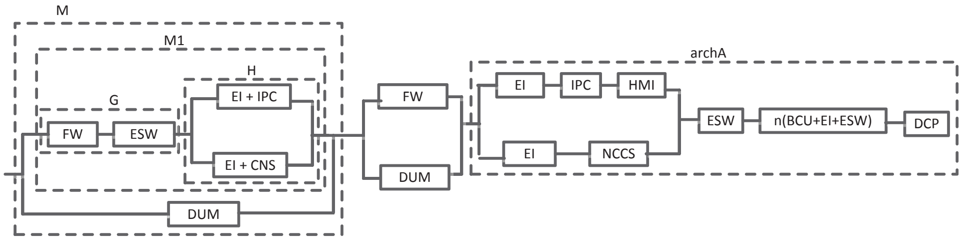


Figure 33: Reliability Block Diagram for Architecture 4

Following equations show the calculation of equivalent failure and repair rates for architecture 4.

Failure rate of M1:

$$\lambda_{\mathrm{M1}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H}} \tag{119}$$

Repair rate of M1:

$$\mu_{\mathrm{M1}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}}(\lambda_{\mathrm{G}} + \lambda_{\mathrm{H}})}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}}) - \mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}}} \tag{120}$$

Failure rate of M:

$$\lambda_{\mathrm{M}} = \frac{\lambda_{\mathrm{M1}} \cdot \lambda_{\mathrm{DUM}}(\mu_{\mathrm{M1}} + \mu_{\mathrm{DUM}})}{(\lambda_{\mathrm{M1}} + \mu_{\mathrm{M1}})(\lambda_{\mathrm{DUM}} + \mu_{\mathrm{DUM}}) - \lambda_{\mathrm{M1}} \cdot \lambda_{\mathrm{DUM}}} \tag{121}$$

Repair rate of M:

$$\mu_{\mathrm{M}} = \mu_{\mathrm{M1}} + \mu_{\mathrm{DUM}} \tag{122}$$

Failure rate of N:

$$\lambda_{\mathrm{N}} = \frac{\lambda_{\mathrm{FW}} \cdot \lambda_{\mathrm{DUM}}(\mu_{\mathrm{FW}} + \mu_{\mathrm{DUM}})}{(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}})(\lambda_{\mathrm{DUM}} + \mu_{\mathrm{DUM}}) - \lambda_{\mathrm{FW}} \cdot \lambda_{\mathrm{DUM}}} \tag{123}$$

Repair rate of N:

$$\mu_{\mathrm{N}} = \mu_{\mathrm{FW}} + \mu_{\mathrm{DUM}} \tag{124}$$

Failure rate of architecture 4:

$$\lambda_{\mathrm{arch4}} = \lambda_{\mathrm{M}} + \lambda_{\mathrm{N}} + \lambda_{\mathrm{archA}} \tag{125}$$

Repair rate of architecture 4:

$$\mu_{\mathrm{arch4}} = \frac{\mu_{\mathrm{M}} \cdot \mu_{\mathrm{N}} \cdot \mu_{\mathrm{archA}}(\lambda_{\mathrm{M}} + \lambda_{\mathrm{N}} + \lambda_{\mathrm{archA}})}{(\lambda_{\mathrm{M}} + \mu_{\mathrm{M}})(\lambda_{\mathrm{N}} + \mu_{\mathrm{N}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}}) - \mu_{\mathrm{M}} \cdot \mu_{\mathrm{N}} \cdot \mu_{\mathrm{archA}}} \tag{126}$$

Mean Time To Failure (MTTF)

MTTF of architecture 4 is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{arch4}} = \frac{1}{\lambda_{\mathrm{arch4}}} \tag{127}$$

Probability of Success (P)

Probability of success of architecture 4 is calculated as follows:

$$P_{\mathrm{s,arch4}} = \frac{\mu_{\mathrm{M}} \cdot \mu_{\mathrm{N}} \cdot \mu_{\mathrm{archA}}}{(\lambda_{\mathrm{M}} + \mu_{\mathrm{M}})(\lambda_{\mathrm{N}} + \mu_{\mathrm{N}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}})} \tag{128}$$

Availability (A)

Availability of architecture 4 is calculated as follows:

$$A_{\mathrm{arch4}} = P_{\mathrm{s,arch4}} \tag{129}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 4.

Failure rate for MTTFF of M1:

$$\lambda_{\mathrm{M1,MTTFF}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}} \tag{130}$$

Repair rate for MTTFF of M1:

$$\mu_{\mathrm{M1,MTTFF}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}}(\lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}})}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H,MTTFF}} + \mu_{\mathrm{H}}) - \mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}}} \tag{131}$$

Failure rate for MTTFF of N:

$$\lambda_{\mathrm{N,MTTFF}} = \frac{\lambda_{\mathrm{FW}} \cdot \lambda_{\mathrm{DUM}}(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}} + \lambda_{\mathrm{DUM}} + \mu_{\mathrm{DUM}})}{(\lambda_{\mathrm{FW}} + \lambda_{\mathrm{DUM}})(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}} + \lambda_{\mathrm{DUM}} + \mu_{\mathrm{DUM}}) + \mu_{\mathrm{FW}} \cdot \mu_{\mathrm{DUM}}} \tag{132}$$

Failure rate for MTTFF of architecture 4:

$$\lambda_{\mathrm{arch4,MTTFF}} = \lambda_{\mathrm{M,MTTFF}} + \lambda_{\mathrm{N,MTTFF}} + \lambda_{\mathrm{archA,MTTFF}} \tag{133}$$

MTTFF of architecture 4:

$$\mathrm{MTTFF}_{\mathrm{arch4}} = \frac{1}{\lambda_{\mathrm{arch4,MTTFF}}} \tag{134}$$

7.1.9 Architecture 5

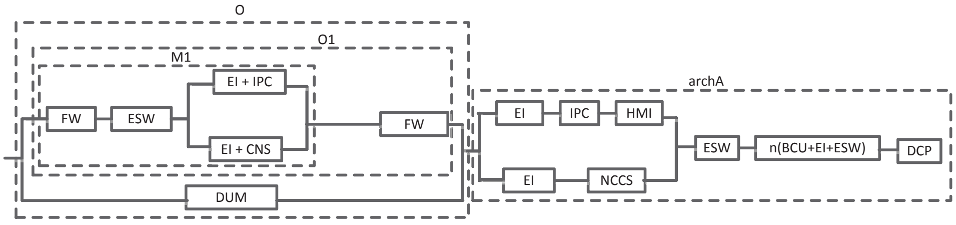


Figure 34: Reliability Block Diagram for Architecture 5

Following equations show the calculation of equivalent failure and repair rates for architecture 5.

Failure rate of O1:

$$\lambda_{\mathrm{O1}} = \lambda_{\mathrm{M1}} + \lambda_{\mathrm{FW}} \tag{135}$$

Repair rate of O1:

$$\mu_{\mathrm{O1}} = \frac{\mu_{\mathrm{M1}} \cdot \mu_{\mathrm{FW}}(\lambda_{\mathrm{M1}} + \lambda_{\mathrm{FW}})}{(\lambda_{\mathrm{M1}} + \mu_{\mathrm{M1}})(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}}) - \mu_{\mathrm{M1}} \cdot \mu_{\mathrm{FW}}} \tag{136}$$

Failure rate of O:

$$\lambda_{\mathrm{O}} = \frac{\lambda_{\mathrm{O1}} \cdot \lambda_{\mathrm{DUM}}(\mu_{\mathrm{O1}} + \mu_{\mathrm{DUM}})}{(\lambda_{\mathrm{O1}} + \mu_{\mathrm{O1}})(\lambda_{\mathrm{DUM}} + \mu_{\mathrm{DUM}}) - \lambda_{\mathrm{O1}} \cdot \lambda_{\mathrm{DUM}}} \tag{137}$$

Repair rate of O:

$$\mu_{\mathrm{O}} = \mu_{\mathrm{O1}} + \mu_{\mathrm{DUM}} \tag{138}$$

Failure rate of architecture 5:

$$\lambda_{\mathrm{arch5}} = \lambda_{\mathrm{O}} + \lambda_{\mathrm{archA}} \tag{139}$$

Repair rate of architecture 5:

$$\mu_{\mathrm{arch5}} = \frac{\mu_{\mathrm{O}} \cdot \mu_{\mathrm{archA}}(\lambda_{\mathrm{O}} + \lambda_{\mathrm{archA}})}{(\lambda_{\mathrm{O}} + \mu_{\mathrm{O}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}}) - \mu_{\mathrm{O}} \cdot \mu_{\mathrm{archA}}} \tag{140}$$

Mean Time To Failure (MTTF)

MTTF of architecture 5 is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{arch5}} = \frac{1}{\lambda_{\mathrm{arch5}}} \tag{141}$$

Probability of Success (P)

Probability of success of architecture 5 is calculated as follows:

$$P_{\mathrm{s,arch5}} = \frac{\mu_{\mathrm{O}} \cdot \mu_{\mathrm{archA}}}{(\lambda_{\mathrm{O}} + \mu_{\mathrm{O}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}})} \tag{142}$$

Availability (A)

Availability of architecture 5 is calculated as follows:

$$A_{\mathrm{arch5}} = P_{\mathrm{s,arch5}} \tag{143}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 5.

Failure rate for MTTFF of O1:

$$\lambda_{\text{O1,MTTFF}} = \lambda_{\text{M1,MTTFF}} + \lambda_{\text{FW}} \tag{144}$$

Repair rate for MTTFF of O1:

$$\mu_{\text{O1,MTTFF}} = \frac{\mu_{\text{M1,MTTFF}} \cdot \mu_{\text{FW}}(\lambda_{\text{M1,MTTFF}} + \lambda_{\text{FW}})}{(\lambda_{\text{M1,MTTFF}} + \mu_{\text{M1,MTTFF}})(\lambda_{\text{FW}} + \mu_{\text{FW}}) - \mu_{\text{M1,MTTFF}} \cdot \mu_{\text{FW}}} \tag{145}$$

Failure rate for MTTFF of architecture 5:

$$\lambda_{\text{arch5,MTTFF}} = \lambda_{\text{O,MTTFF}} + \lambda_{\text{archA,MTTFF}} \tag{146}$$

Repair rate for MTTFF of architecture 5:

$$\text{MTTFF}_{\text{arch5}} = \frac{1}{\lambda_{\text{arch5,MTTFF}}} \tag{147}$$

7.1.10 Architecture 6

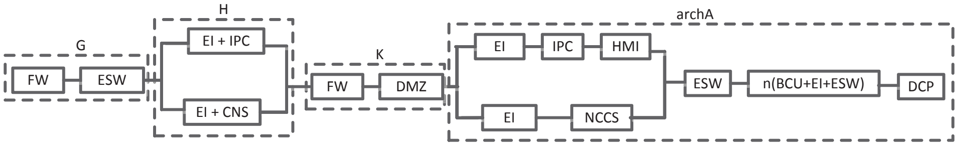


Figure 35: Reliability Block Diagram for Architecture 6

Following equations show the calculation of equivalent failure and repair rates for architecture 6.

Failure rate of K:

$$\lambda_{\text{K}} = \lambda_{\text{FW}} + \lambda_{\text{DMZ}} \tag{148}$$

Repair rate of K:

$$\mu_{\text{K}} = \frac{\mu_{\text{FW}} \cdot \mu_{\text{DMZ}}(\lambda_{\text{FW}} + \lambda_{\text{DMZ}})}{(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{DMZ}} + \mu_{\text{DMZ}}) - \mu_{\text{FW}} \cdot \mu_{\text{DMZ}}} \tag{149}$$

Failure rate of architecture 6:

$$\lambda_{\text{arch6}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{K}} + \lambda_{\text{archA}} \tag{150}$$

Repair rate of architecture 6:

$$\mu_{\text{arch6}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{K}} \cdot \mu_{\text{archA}}(\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{K}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{K}} + \mu_{\text{K}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{K}} \cdot \mu_{\text{archA}}} \tag{151}$$

Mean Time To Failure (MTTF)

MTTF of architecture 6 is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{arch6}} = \frac{1}{\lambda_{\mathrm{arch6}}} \tag{152}$$

Probability of Success (P)

Probability of success of architecture 6 is calculated as follows:

$$P_{\mathrm{s,arch6}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{K}} \cdot \mu_{\mathrm{archA}}}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}})(\lambda_{\mathrm{K}} + \mu_{\mathrm{K}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}})} \tag{153}$$

Availability (A)

Availability of architecture 6 is calculated as follows:

$$A_{\mathrm{arch6}} = P_{\mathrm{s,arch6}} \tag{154}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 6.

Failure rate for MTTFF of architecture 6:

$$\lambda_{\mathrm{arch6,MTTFF}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}} + \lambda_{\mathrm{K}} + \lambda_{\mathrm{archA,MTTFF}} \tag{155}$$

MTTFF of architecture 6:

$$\mathrm{MTTFF}_{\mathrm{arch6}} = \frac{1}{\lambda_{\mathrm{arch6,MTTFF}}} \tag{156}$$

7.1.11 Architecture 7

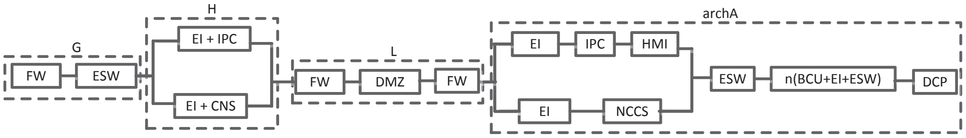


Figure 36: Reliability Block Diagram for Architecture 7

Following equations show the calculation of equivalent failure and repair rates for architecture 7.

Failure rate of L:

$$\lambda_{\mathrm{L}} = \lambda_{\mathrm{FW}} + \lambda_{\mathrm{DMZ}} + \lambda_{\mathrm{FW}} \tag{157}$$

Repair rate of L:

$$\mu_{\mathrm{L}} = \frac{\mu_{\mathrm{FW}}^2 \cdot \mu_{\mathrm{DMZ}}(2\lambda_{\mathrm{FW}} + \lambda_{\mathrm{DMZ}})}{(\lambda_{\mathrm{FW}} + \mu_{\mathrm{FW}})^2(\lambda_{\mathrm{DMZ}} + \mu_{\mathrm{DMZ}}) - \mu_{\mathrm{FW}}^2 \cdot \mu_{\mathrm{DMZ}}} \tag{158}$$

Failure rate of architecture 7:

$$\lambda_{\mathrm{arch7}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H}} + \lambda_{\mathrm{L}} + \lambda_{\mathrm{archA}} \tag{159}$$

Repair rate of architecture 7:

$$\mu_{\mathrm{arch7}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{L}} \cdot \mu_{\mathrm{archA}}(\lambda_{\mathrm{G}} + \lambda_{\mathrm{H}} + \lambda_{\mathrm{L}} + \lambda_{\mathrm{archA}})}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}})(\lambda_{\mathrm{L}} + \mu_{\mathrm{L}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}}) - \mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{L}} \cdot \mu_{\mathrm{archA}}} \tag{160}$$

Mean Time To Failure (MTTF)

MTTF of architecture 7 is calculated as follows:

$$\mathrm{MTTF}_{\mathrm{arch7}} = \frac{1}{\lambda_{\mathrm{arch7}}} \tag{161}$$

Probability of Success (P)

Probability of success of architecture 7 is calculated as follows:

$$P_{\mathrm{s,arch7}} = \frac{\mu_{\mathrm{G}} \cdot \mu_{\mathrm{H}} \cdot \mu_{\mathrm{L}} \cdot \mu_{\mathrm{archA}}}{(\lambda_{\mathrm{G}} + \mu_{\mathrm{G}})(\lambda_{\mathrm{H}} + \mu_{\mathrm{H}})(\lambda_{\mathrm{L}} + \mu_{\mathrm{L}})(\lambda_{\mathrm{archA}} + \mu_{\mathrm{archA}})} \tag{162}$$

Availability (A)

Availability of architecture 7 is calculated as follows:

$$A_{\mathrm{arch7}} = P_{\mathrm{s,arch7}} \tag{163}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 7.

Failure rate for MTTFF of architecture 7:

$$\lambda_{\mathrm{arch7,MTTFF}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}} + \lambda_{\mathrm{L}} + \lambda_{\mathrm{archA,MTTFF}} \tag{164}$$

MTTFF of architecture 7:

$$\mathrm{MTTFF}_{\mathrm{arch7}} = \frac{1}{\lambda_{\mathrm{arch7,MTTFF}}} \tag{165}$$

7.1.12 Architecture 8

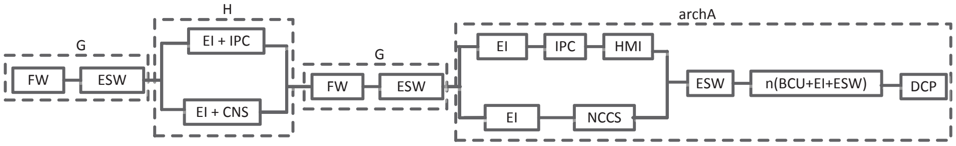


Figure 37: Reliability Block Diagram for Architecture 8

Following equations show the calculation of equivalent failure and repair rates for architecture 8.

Failure rate of architecture 8:

$$\lambda_{\text{arch8}} = 2\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{archA}} \tag{166}$$

Repair rate of architecture 8:

$$\mu_{\text{arch8}} = \frac{\mu_{\text{G}}^2 \cdot \mu_{\text{H}} \cdot \mu_{\text{archA}}(2\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})^2(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}}^2 \cdot \mu_{\text{H}} \cdot \mu_{\text{archA}}} \tag{167}$$

Mean Time To Failure (MTTF)

MTTF of architecture 8 is calculated as follows:

$$\text{MTTF}_{\text{arch8}} = \frac{1}{\lambda_{\text{arch8}}} \tag{168}$$

Probability of Success (P)

Probability of success of architecture 8 is calculated as follows:

$$P_{\text{s,arch8}} = \frac{\mu_{\text{G}}^2 \cdot \mu_{\text{H}} \cdot \cdot \mu_{\text{archA}}}{(\lambda_{\text{G}} + \mu_{\text{G}})^2(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{archA}} + \mu_{\text{archA}})} \tag{169}$$

Availability (A)

Availability of architecture 8 is calculated as follows:

$$A_{\text{arch8}} = P_{\text{s,arch8}} \tag{170}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 8.

Failure rate for MTTFF of architecture 8:

$$\lambda_{\text{arch8,MTTFF}} = 2\lambda_{\text{G}} + \lambda_{\text{H,MTTFF}} + \lambda_{\text{archA,MTTFF}} \tag{171}$$

MTTFF of architecture 8:

$$\text{MTTFF}_{\text{arch8}} = \frac{1}{\lambda_{\text{arch8,MTTFF}}} \tag{172}$$

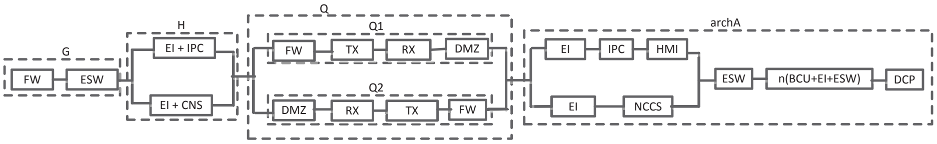


Figure 38: Reliability Block Diagram for Architecture 9

7.1.13 Architecture 9

Following equations show the calculation of equivalent failure and repair rates for architecture 9.

Failure rate of Q1:

$$\lambda_{\text{Q1}} = \lambda_{\text{FW}} + \lambda_{\text{TX}} + \lambda_{\text{RX}} + \lambda_{\text{DMZ}} \tag{173}$$

Repair rate of Q1:

$$\mu_{\text{Q1}} = \frac{\mu_{\text{FW}} \cdot \mu_{\text{TX}} \cdot \mu_{\text{RX}} \cdot \mu_{\text{DMZ}}(\lambda_{\text{FW}} + \lambda_{\text{TX}} + \lambda_{\text{RX}} + \lambda_{\text{DMZ}})}{(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{TX}} + \mu_{\text{TX}})(\lambda_{\text{RX}} + \mu_{\text{RX}})(\lambda_{\text{DMZ}} + \mu_{\text{DMZ}}) - \mu_{\text{FW}} \cdot \mu_{\text{TX}} \cdot \mu_{\text{RX}} \cdot \mu_{\text{DMZ}}} \tag{174}$$

Failure rate of Q2:

$$\lambda_{\text{Q2}} = \lambda_{\text{Q1}} \tag{175}$$

Repair rate of Q2:

$$\mu_{\text{Q2}} = \mu_{\text{Q1}} \tag{176}$$

Failure rate of Q:

$$\lambda_{\text{Q}} = \frac{2\lambda_{\text{Q1}}^2 \cdot \mu_{\text{Q1}}}{(\lambda_{\text{Q1}} + \mu_{\text{Q1}})^2 - \lambda_{\text{Q1}}^2} \tag{177}$$

Repair rate of Q:

$$\mu_{\text{Q}} = 2\mu_{\text{Q1}} \tag{178}$$

Failure rate of architecture 9:

$$\lambda_{\text{arch9}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{Q}} + \lambda_{\text{archA}} \tag{179}$$

Repair rate of architecture 9:

$$\mu_{\text{arch9}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{Q}} \cdot \mu_{\text{archA}}(\lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{Q}} + \lambda_{\text{archA}})}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{Q}} + \mu_{\text{Q}})(\lambda_{\text{archA}} + \mu_{\text{archA}}) - \mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{Q}} \cdot \mu_{\text{archA}}} \tag{180}$$

Mean Time To Failure (MTTF)

MTTF of architecture 9 is calculated as follows:

$$\text{MTTF}_{\text{arch9}} = \frac{1}{\lambda_{\text{arch9}}} \tag{181}$$

Probability of Success (P)

Probability of success of architecture 9 is calculated as follows:

$$P_{\text{s,arch9}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{Q}} \cdot \mu_{\text{archA}}}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{Q}} + \mu_{\text{Q}})(\lambda_{\text{archA}} + \mu_{\text{archA}})} \tag{182}$$

Availability (A)

Availability of architecture 9 is calculated as follows:

$$A_{\text{arch9}} = P_{\text{s,arch9}} \tag{183}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 9.

Failure rate for MTTFF of Q:

$$\lambda_{\text{Q,MTTFF}} = \frac{\lambda_{\text{Q1}} \cdot \lambda_{\text{Q2}}(\lambda_{\text{Q1}} + \mu_{\text{Q1}} + \lambda_{\text{Q2}} + \mu_{\text{Q2}})}{(\lambda_{\text{Q1}} + \lambda_{\text{Q2}})(\lambda_{\text{Q1}} + \mu_{\text{Q1}} + \lambda_{\text{Q2}} + \mu_{\text{Q2}}) + \mu_{\text{Q1}} \cdot \mu_{\text{Q2}}} \tag{184}$$

Failure rate for MTTFF of architecture 9:

$$\lambda_{\text{arch9,MTTFF}} = \lambda_{\text{G}} + \lambda_{\text{H,MTTFF}} + \lambda_{\text{Q,MTTF}} + \lambda_{\text{archA,MTTFF}} \tag{185}$$

MTTFF of architecture 9:

$$\text{MTTFF}_{\text{arch9}} = \frac{1}{\lambda_{\text{arch9,MTTFF}}} \tag{186}$$

7.1.14 Architecture 10

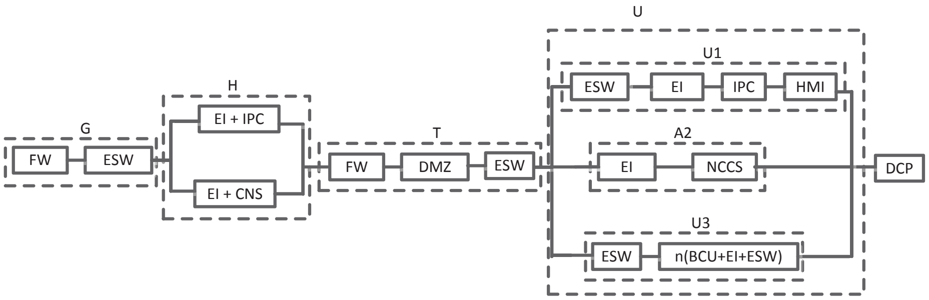


Figure 39: Reliability Block Diagram for Architecture 10

Following equations show the calculation of equivalent failure and repair rates for architecture 10.

Failure rate of T:

$$\lambda_{\text{T}} = \lambda_{\text{FW}} + \lambda_{\text{DMZ}} + \lambda_{\text{ESW}} \tag{187}$$

Repair rate of T:

$$\mu_{\text{T}} = \frac{\mu_{\text{FW}} \cdot \mu_{\text{DMZ}} \cdot \mu_{\text{ESW}}(\lambda_{\text{FW}} + \lambda_{\text{DMZ}} + \lambda_{\text{ESW}})}{(\lambda_{\text{FW}} + \mu_{\text{FW}})(\lambda_{\text{DMZ}} + \mu_{\text{DMZ}})(\lambda_{\text{ESW}} + \mu_{\text{ESW}}) - \mu_{\text{FW}} \cdot \mu_{\text{DMZ}} \cdot \mu_{\text{ESW}}} \tag{188}$$

Failure rate of U1:

$$\lambda_{\text{U1}} = \lambda_{\text{ESW}} + \lambda_{\text{EI}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}} \tag{189}$$

Repair rate of U1:

$$\mu_{\text{U1}} = \frac{\mu_{\text{ESW}} \cdot \mu_{\text{EI}} \cdot \mu_{\text{IPC}} \cdot \mu_{\text{HMI}}(\lambda_{\text{ESW}} + \lambda_{\text{EI}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}})}{(\lambda_{\text{ESW}} + \mu_{\text{ESW}})(\lambda_{\text{EI}} + \mu_{\text{EI}})(\lambda_{\text{IPC}} + \mu_{\text{IPC}})(\lambda_{\text{HMI}} + \mu_{\text{HMI}}) - \mu_{\text{ESW}} \cdot \mu_{\text{EI}} \cdot \mu_{\text{IPC}} \cdot \mu_{\text{HMI}}} \tag{190}$$

Failure rate of U3:

$$\lambda_{\text{U3}} = \lambda_{\text{B}} + \lambda_{\text{ESW}} \tag{191}$$

Repair rate of U3:

$$\mu_{\text{U3}} = \frac{\mu_{\text{ESW}} \cdot \mu_{\text{B}}(\lambda_{\text{ESW}} + \lambda_{\text{B}})}{(\lambda_{\text{ESW}} + \mu_{\text{ESW}})(\lambda_{\text{B}} + \mu_{\text{B}}) - \mu_{\text{ESW}} \cdot \mu_{\text{B}}} \tag{192}$$

Failure rate of U:

$$\lambda_{\text{U}} = \frac{\lambda_{\text{U1}} \cdot \lambda_{\text{A2}} \cdot \lambda_{\text{U3}}(\mu_{\text{U1}} + \mu_{\text{A2}} + \mu_{\text{U3}})}{(\lambda_{\text{U1}} + \mu_{\text{U1}})(\lambda_{\text{A2}} + \mu_{\text{A2}})(\lambda_{\text{U3}} + \mu_{\text{U3}}) - \lambda_{\text{U1}} \cdot \lambda_{\text{A2}} \cdot \lambda_{\text{U3}}} \tag{193}$$

Repair rate of U:

$$\mu_{\text{U}} = \mu_{\text{U1}} + \mu_{\text{A2}} + \mu_{\text{U3}} \tag{194}$$

Failure rate of architecture 10:

$$\lambda_{\text{arch10}} = \lambda_{\text{G}} + \lambda_{\text{H}} + \lambda_{\text{T}} + \lambda_{\text{U}} + \lambda_{\text{DCP}} \tag{195}$$

Mean Time To Failure (MTTF)

MTTF of architecture 10 is calculated as follows:

$$\text{MTTF}_{\text{arch10}} = \frac{1}{\lambda_{\text{arch10}}} \tag{196}$$

Probability of Success (P)

Probability of success of architecture 10 is calculated as follows:

$$P_{\text{s,arch10}} = \frac{\mu_{\text{G}} \cdot \mu_{\text{H}} \cdot \mu_{\text{T}} \cdot \mu_{\text{U}} \cdot \mu_{\text{DCP}}}{(\lambda_{\text{G}} + \mu_{\text{G}})(\lambda_{\text{H}} + \mu_{\text{H}})(\lambda_{\text{T}} + \mu_{\text{T}})(\lambda_{\text{U}} + \mu_{\text{U}})(\lambda_{\text{DCP}} + \mu_{\text{DCP}})} \tag{197}$$

Availability (A)

Availability of architecture 10 is calculated as follows:

$$A_{\text{arch10}} = P_{\text{s,arch10}} \tag{198}$$

Mean Time To First Failure (MTTFF)

Following equations show the calculation of MTTFF for architecture 10.

Failure rate for MTTFF of U:

$$\lambda_{\mathrm{U,MTTFF}} = \frac{\lambda_{\mathrm{U1}} \cdot \lambda_{\mathrm{A2}} \cdot \lambda_{\mathrm{U3}}(\lambda_{\mathrm{U1}} + \mu_{\mathrm{U1}} + \lambda_{\mathrm{A2}} + \mu_{\mathrm{A2}} + \lambda_{\mathrm{U3}} + \mu_{\mathrm{U3}})}{(\lambda_{\mathrm{U1}} + \lambda_{\mathrm{A2}} + \lambda_{\mathrm{U3}})(\lambda_{\mathrm{U1}} + \mu_{\mathrm{U1}} + \lambda_{\mathrm{A2}} + \mu_{\mathrm{A2}} + \lambda_{\mathrm{U3}} + \mu_{\mathrm{U3}}) + \mu_{\mathrm{U1}} \cdot \mu_{\mathrm{A2}} \cdot \mu_{\mathrm{U3}}} \tag{199}$$

Failure rate for MTTFF of architecture 10:

$$\lambda_{\mathrm{arch10,MTTFF}} = \lambda_{\mathrm{G}} + \lambda_{\mathrm{H,MTTFF}} + \lambda_{\mathrm{T}} + \lambda_{\mathrm{U,MTTFF}} + \lambda_{\mathrm{DCP}} \tag{200}$$

MTTFF of architecture 10:

$$\mathrm{MTTFF}_{\mathrm{arch10}} = \frac{1}{\lambda_{\mathrm{arch10,MTTFF}}} \tag{201}$$

7.2 Non-Repairable System Model

This section presents the mathematical model for calculating reliability and MTTF of architectures A to D and reliability of architectures 1-10 for non-repairable system model.

7.2.1 Reliability: Architecture A

Following equations show the calculation of reliability for architecture A.

Probability of success of A1:

$$P_{\mathrm{A1}} = P_{\mathrm{EI}} \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} \tag{202}$$

Probability of success of A2:

$$P_{\mathrm{A2}} = P_{\mathrm{EI}} \cdot P_{\mathrm{NCCS}} \tag{203}$$

Probability of success of A:

$$\begin{aligned} P_{\mathrm{A}} &= 1 - (1 - P_{\mathrm{A1}})(1 - P_{\mathrm{A2}}) && (204) \\ &= P_{\mathrm{A1}} + P_{\mathrm{A2}} - P_{\mathrm{A1}} \cdot P_{\mathrm{A2}} && (205) \end{aligned}$$

Probability of success of B:

$$P_{\mathrm{B}} = P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^2 \cdot P_{\mathrm{ESW}}^2 \tag{206}$$

Reliability of architecture A:

$$R_{\mathrm{archA}} = P_{\mathrm{archA}} = P_{\mathrm{DCP}} \cdot P_{\mathrm{B}} \cdot P_{\mathrm{ESW}} \cdot P_{\mathrm{A}} \tag{207}$$

$$R_{\mathrm{archA}} = P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^2 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{ESW}}(P_{\mathrm{EI}} \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} + P_{\mathrm{EI}} \cdot P_{\mathrm{NCCS}} - P_{\mathrm{EI}}^2 \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} P_{\mathrm{NCCS}}) \tag{208}$$

$$R_{\mathrm{archA}} = P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^3 [P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}}(1 - P_{\mathrm{EI}} \cdot P_{\mathrm{NCCS}}) + P_{\mathrm{NCCS}}] \tag{209}$$

Mean Time To Failure (MTTF)

MTTF for architecture A is calculated as follows.

Reliability of architecture A in expanded form:

$$\begin{aligned} R_{\text{archA}} =& P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^3 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \\ & - P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^4 \cdot P_{\text{ESW}}^3 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \cdot P_{\text{NCCS}} \\ & + P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^3 \cdot P_{\text{NCCS}} \end{aligned} \tag{210}$$

MTTF of architecture A:

$$\begin{aligned} \text{MTTF}_{\text{archA}} =& \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{ESW}} + 3\lambda_{\text{EI}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}}} \\ & + \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{ESW}} + 3\lambda_{\text{EI}} + \lambda_{\text{NCCS}}} \\ & - \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{ESW}} + 4\lambda_{\text{EI}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}} + \lambda_{\text{NCCS}}} \end{aligned} \tag{211}$$

7.2.2 Reliability: Architecture B

Following equations show the calculation of reliability for architecture B.

Probability of success of C1:

$$P_{\text{C1}} = P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \tag{212}$$

Probability of success of C2:

$$P_{\text{C2}} = P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{NCCS}} \tag{213}$$

Probability of success of C:

$$P_{\text{C}} = P_{\text{C1}} + P_{\text{C2}} - P_{\text{C1}} \cdot P_{\text{C2}} \tag{214}$$

Probability of success of D:

$$P_{\text{D}} = P_{\text{BCU}}^2 \cdot P_{\text{EI}}^2 \tag{215}$$

Reliability of architecture B:

$$R_{\text{archB}} = P_{\text{archB}} = P_{\text{DCP}} \cdot P_{\text{D}} \cdot P_{\text{ESW}} \cdot P_{\text{C}} \tag{216}$$

$$\begin{aligned} R_{\text{archB}} =& P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^2 \cdot P_{\text{ESW}}(P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \\ & + P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{NCCS}} - P_{\text{ESW}}^2 \cdot P_{\text{EI}}^2 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} P_{\text{NCCS}}) \end{aligned} \tag{217}$$

$$R_{\text{archB}} = P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^2 [P_{\text{IPC}} \cdot P_{\text{HMI}}(1 - P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{NCCS}}) + P_{\text{NCCS}}] \tag{218}$$

Mean Time To Failure (MTTF)

MTTF for architecture B is calculated as follows.

Reliability of architecture B in expanded form:

$$\begin{aligned}R_{\mathrm{archB}} =& P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} \\ &- P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^4 \cdot P_{\mathrm{ESW}}^3 \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} \cdot P_{\mathrm{NCCS}} \\ &+ P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{NCCS}}\end{aligned} \tag{219}$$

MTTF of architecture B:

$$\begin{aligned}\mathrm{MTTF}_{\mathrm{archB}} =& \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 3\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}}} \\ &+ \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 3\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{NCCS}}} \\ &- \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 4\lambda_{\mathrm{EI}} + 3\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}} + \lambda_{\mathrm{NCCS}}}\end{aligned} \tag{220}$$

7.2.3 Reliability: Architecture C

Following equations show the calculation of reliability for architecture C.

Reliability of architecture C:

$$R_{\mathrm{archC}} = P_{\mathrm{archC}} = P_{\mathrm{DCP}} \cdot P_{\mathrm{D}} \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{A}} \tag{221}$$

$$R_{\mathrm{archC}} = P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^2 [P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}}(1 - P_{\mathrm{EI}} \cdot P_{\mathrm{NCCS}}) + P_{\mathrm{NCCS}}] \tag{222}$$

Mean Time To Failure (MTTF)

MTTF for architecture C is calculated as follows.

Reliability of architecture C in expanded form:

$$\begin{aligned}R_{\mathrm{archC}} =& P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} \\ &- P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^4 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{IPC}} \cdot P_{\mathrm{HMI}} \cdot P_{\mathrm{NCCS}} \\ &+ P_{\mathrm{DCP}} \cdot P_{\mathrm{BCU}}^2 \cdot P_{\mathrm{EI}}^3 \cdot P_{\mathrm{ESW}}^2 \cdot P_{\mathrm{NCCS}}\end{aligned} \tag{223}$$

MTTF of architecture C:

$$\begin{aligned}\mathrm{MTTF}_{\mathrm{archC}} =& \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 3\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}}} \\ &+ \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 3\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{NCCS}}} \\ &- \frac{1}{\lambda_{\mathrm{DCP}} + 2\lambda_{\mathrm{BCU}} + 4\lambda_{\mathrm{EI}} + 2\lambda_{\mathrm{ESW}} + \lambda_{\mathrm{IPC}} + \lambda_{\mathrm{HMI}} + \lambda_{\mathrm{NCCS}}}\end{aligned} \tag{224}$$

7.2.4 Reliability: Architecture D

Following equations show the calculation of reliability for architecture D.

Probability of success of F1:

$$P_{\text{F1}} = P_{\text{ESW}}^2 \tag{225}$$

Probability of success of F:

$$\begin{aligned} P_{\text{F}} &= 1 - (1 - P_{\text{F1}})^2 && (226) \\ &= P_{\text{ESW}}^2(2 - P_{\text{ESW}}^2) && (227) \end{aligned}$$

Reliability of architecture D:

$$R_{\text{archD}} = P_{\text{archD}} = P_{\text{DCP}} \cdot P_{\text{D}} \cdot P_{\text{F}} \cdot P_{\text{A}} \tag{228}$$

$$R_{\text{archD}} = P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^2 \cdot P_{\text{ESW}}^2(2 - P_{\text{ESW}}^2) P_{\text{EI}}[P_{\text{IPC}} \cdot P_{\text{HMI}}(1 - P_{\text{EI}} \cdot P_{\text{NCCS}}) + P_{\text{NCCS}}] \tag{229}$$

$$R_{\text{archD}} = P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^2(2 - P_{\text{ESW}}^2)[P_{\text{IPC}} \cdot P_{\text{HMI}}(1 - P_{\text{EI}} \cdot P_{\text{NCCS}}) + P_{\text{NCCS}}] \tag{230}$$

Mean Time To Failure (MTTF)

MTTF for architecture D is calculated as follows.

Reliability of architecture D in expanded form:

$$\begin{aligned} R_{\text{archD}} =& 2P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^2 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \\ &+ 2P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^2 \cdot P_{\text{NCCS}} \\ &- 2P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^4 \cdot P_{\text{ESW}}^2 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \cdot P_{\text{NCCS}} \\ &- P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^4 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \\ &- P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^3 \cdot P_{\text{ESW}}^4 \cdot P_{\text{NCCS}} \\ &+ P_{\text{DCP}} \cdot P_{\text{BCU}}^2 \cdot P_{\text{EI}}^4 \cdot P_{\text{ESW}}^4 \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \cdot P_{\text{NCCS}} \end{aligned} \tag{231}$$

MTTF of architecture D:

$$\begin{aligned} \text{MTTF}_{\text{archD}} =& \frac{2}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{EI}} + 2\lambda_{\text{ESW}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}}} \\ &+ \frac{2}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{EI}} + 2\lambda_{\text{ESW}} + \lambda_{\text{NCCS}}} \\ &- \frac{2}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 4\lambda_{\text{EI}} + 2\lambda_{\text{ESW}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}} + \lambda_{\text{NCCS}}} \\ &- \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{EI}} + 4\lambda_{\text{ESW}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}}} \\ &- \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 3\lambda_{\text{EI}} + 4\lambda_{\text{ESW}} + \lambda_{\text{NCCS}}} \\ &- \frac{1}{\lambda_{\text{DCP}} + 2\lambda_{\text{BCU}} + 4\lambda_{\text{EI}} + 4\lambda_{\text{ESW}} + \lambda_{\text{IPC}} + \lambda_{\text{HMI}} + \lambda_{\text{NCCS}}} \end{aligned} \tag{232}$$

7.2.5 Reliability: Architecture 1

Following equations show the calculation of reliability for architecture 1.

Probability of success of G:

$$P_{\mathrm{G}} = P_{\mathrm{FW}} \cdot P_{\mathrm{ESW}} \tag{233}$$

Probability of success of H1:

$$P_{\mathrm{H1}} = P_{\mathrm{EI}} \cdot P_{\mathrm{IPC}} \tag{234}$$

Probability of success of H2:

$$P_{\mathrm{H2}} = P_{\mathrm{EI}} \cdot P_{\mathrm{CNS}} \tag{235}$$

Probability of success of H:

$$P_{\mathrm{H}} = P_{\mathrm{H1}} + P_{\mathrm{H2}} - P_{\mathrm{H1}} \cdot P_{\mathrm{H2}} \tag{236}$$

Probability of success of J:

$$P_{\mathrm{J}} = 2P_{\mathrm{DHC}} - P_{\mathrm{DHC}}^{2} \tag{237}$$

Reliability of architecture 1:

$$R_{\mathrm{arch1}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{J}} \cdot P_{\mathrm{archA}} \tag{238}$$

7.2.6 Reliability: Architecture 2

Reliability of architecture 2 is calculated as follows:

$$R_{\mathrm{arch2}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{DHS}} \cdot P_{\mathrm{archA}} \tag{239}$$

7.2.7 Reliability: Architecture 3

Reliability of architecture 2 is calculated as follows:

$$R_{\mathrm{arch3}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{FW}} \cdot P_{\mathrm{archA}} \tag{240}$$

7.2.8 Reliability: Architecture 4

Following equations show the calculation of reliability for architecture 4.

Probability of success of M1:

$$P_{\mathrm{M1}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \tag{241}$$

Probability of success of M:

$$P_{\mathrm{M}} = P_{\mathrm{M1}} + P_{\mathrm{DUM}} - P_{\mathrm{M1}} \cdot P_{\mathrm{DUM}} \tag{242}$$

Probability of success of N:

$$P_{\mathrm{N}} = P_{\mathrm{FW}} + P_{\mathrm{DUM}} - P_{\mathrm{FW}} \cdot P_{\mathrm{DUM}} \tag{243}$$

Reliability of architecture 4:

$$R_{\mathrm{arch4}} = P_{\mathrm{M}} \cdot P_{\mathrm{N}} \cdot P_{\mathrm{archA}} \tag{244}$$

7.2.9 Reliability: Architecture 5

Following equations show the calculation of reliability for architecture 5.

Probability of success of O1:

$$P_{\mathrm{O1}} = P_{\mathrm{M1}} \cdot P_{\mathrm{FW}} \tag{245}$$

Probability of success of O:

$$P_{\mathrm{O}} = P_{\mathrm{O1}} + P_{\mathrm{DUM}} - P_{\mathrm{O1}} \cdot P_{\mathrm{DUM}} \tag{246}$$

Reliability of architecture 5:

$$R_{\mathrm{arch5}} = P_{\mathrm{O}} \cdot P_{\mathrm{archA}} \tag{247}$$

7.2.10 Reliability: Architecture 6

Following equations show the calculation of reliability for architecture 6.

Probability of success of K:

$$P_{\mathrm{K}} = P_{\mathrm{FW}} \cdot P_{\mathrm{DMZ}} \tag{248}$$

Reliability of architecture 6:

$$R_{\mathrm{arch6}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{K}} \cdot P_{\mathrm{archA}} \tag{249}$$

7.2.11 Reliability: Architecture 7

Following equations show the calculation of reliability for architecture 7.

Probability of success of L:

$$P_{\mathrm{L}} = P_{\mathrm{FW}}^2 \cdot P_{\mathrm{DMZ}} \tag{250}$$

Reliability of architecture 7:

$$R_{\mathrm{arch7}} = P_{\mathrm{G}} \cdot P_{\mathrm{H}} \cdot P_{\mathrm{L}} \cdot P_{\mathrm{archA}} \tag{251}$$

7.2.12 Reliability: Architecture 8

Following equations show the calculation of reliability for architecture 8.

$$R_{\mathrm{arch8}} = P_{\mathrm{G}}^2 \cdot P_{\mathrm{H}} \cdot P_{\mathrm{archA}} \tag{252}$$

7.2.13 Reliability: Architecture 9

Following equations show the calculation of reliability for architecture 9.

Probability of success of Q1:

$$P_{\mathrm{Q1}} = P_{\mathrm{FW}} \cdot P_{\mathrm{TX}} \cdot P_{\mathrm{RX}} \cdot P_{\mathrm{DMZ}} \tag{253}$$

Probability of success of Q2:

$$P_{\mathrm{Q2}} = P_{\mathrm{Q1}} \tag{254}$$

Probability of success of Q:

$$P_{\text{Q}} = 2P_{\text{Q1}} - P_{\text{Q1}}^2 \tag{255}$$

Reliability of architecture 9:

$$R_{\text{arch9}} = P_{\text{G}} \cdot P_{\text{H}} \cdot P_{\text{Q}} \cdot P_{\text{archA}} \tag{256}$$

7.2.14 Reliability: Architecture 10

Following equations show the calculation of reliability for architecture 10.

Probability of success of T:

$$P_{\text{T}} = P_{\text{FW}} \cdot P_{\text{DMZ}} \cdot P_{\text{ESW}} \tag{257}$$

Probability of success of U1:

$$P_{\text{U1}} = P_{\text{ESW}} \cdot P_{\text{EI}} \cdot P_{\text{IPC}} \cdot P_{\text{HMI}} \tag{258}$$

Probability of success of U3:

$$P_{\text{U3}} = P_{\text{ESW}} \cdot P_{\text{B}} \tag{259}$$

Probability of success of U:

$$P_{\text{U}} = 1 - (1 - P_{\text{U1}})(1 - P_{\text{A2}})(1 - P_{\text{U3}}) \tag{260}$$

Reliability of architecture 10:

$$R_{\text{arch10}} = P_{\text{G}} \cdot P_{\text{H}} \cdot P_{\text{T}} \cdot P_{\text{U}} \cdot P_{\text{DCP}} \tag{261}$$