Strategic Redundancy for Improved System Reliability and Cost-Efficiency

Vartika T Rao
Information Technology
National Institute of Technology
Karnataka, India
vartikatrao.211it077@nitk.edu.in

Shubham Subodh Rasal
Information Technology
National Institute of Technology
Karnataka, India
shubham.211it066@nitk.edu.in

Soumya Sangam Jha
Information Technology
National Institute of Technology
Karnataka, India
soumyajha.211it068@nitk.edu.in

Subhojit Karmakar
Information Technology
National Institute of Technology
Karnataka, India
subhojit.211it071@nitk.edu.in

Biju R. Mohan
Information Technology
National Institute of Technology
Karnataka, India
biju@nitk.edu.in

Madhusmita Das
Information Technology
National Institute of Technology
Karnakata, India
madhusmitadas.197it004@nitk.edu.in

***Abstract*—A safety-critical system is a type of system whose failure can cause catastrophic consequences, such as loss of life, significant environmental damage, or severe financial losses. These systems demand high levels of reliability as they are designed and operated with the primary goal of ensuring the safety of individuals and the surrounding environment. In this paper, we provide a systematic and data-driven approach to improve the reliability of an Automatic Fire Sprinkler System (AFSS) with limited economic resources by strategically adding back-ups to the key system components. We use Fault Tree Analysis (FTA) to identify the components potentially leading to system failures and assess the benefits of adding backup based on their Redundancy Benefit(RB). Formal specification and verification of the new system with added redundancy is performed using the Temporal Logic of Actions (TLA+) tool and parsed through the TLC model checker to justify the correctness of the specifications.**

***Index Terms*—Safety-critical system (SCS), Redundancy Benefit (RB), Cost Efficiency, Fault Tree Analysis (FTA), Temporal Logic Of Actions (TLA+) tool, TLC Model Checker, Temporal equivalence**

I. Introduction

Safety-critical systems are indispensable in safeguarding human lives, preserving the environment, and averting catastrophic financial losses. These systems, by design, operate with the primary goal of ensuring the safety of individuals and the surrounding environment. Enhancing their reliability is paramount, given the high stakes associated with safety-critical systems. Thus, reliability analysis and fault assessment are pivotal in ensuring these systems operate flawlessly, especially when lives are at stake.

One such safety-critical system that requires unwavering reliability is the Automatic Fire Sprinkler System (AFSS). These systems are designed to respond swiftly and effectively to fire incidents, with their successful operation often being the thin line between life and death. AFSS consists of various components, such as valves, nozzles, and control systems, all of which must work seamlessly to suppress fires. However, the reliability of these systems can be influenced by the inherent limitations of individual components, making them prime candidates for improvements in reliability through the introduction of redundancy. [1]

Redundancy, in the context of critical systems, refers to incorporating backup components or mechanisms that can take over in the event of primary component failure. This redundancy serves as a fail-safe mechanism, reducing the likelihood of system failure and enhancing overall reliability. Yet, when implementing redundancy, it is crucial to ensure that additional components are added and seamlessly integrated into the system without introducing unintended behaviors or vulnerabilities. [2]

In this paper, we devise a systematic method to add redundancy to the system and model the use of Fault Tree Analysis (FTA) to assess the benefits of the added redundancy. We then use the Temporal Logic of Action (TLA+), which offers a formal and rigorous approach to specifying and verifying the behavior of complex systems[3]. By applying TLA+ to the intermediate system, we can ensure that the added redundancy functions as intended without introducing unintended behaviors or vulnerabilities. This formal analysis provides mathematical proof of the system's correctness, which is paramount in safety-critical systems.

However, the addition of redundancy within the system incurs costs. This cost is also important in assessing whether the benefits from the improved reliability outweigh the financial investments made.

The rest of this paper is organized as follows. Section II discusses the background and related works. Section III describes the methodology. Section IV contains the experimentation. Section V discusses the results, Section VI contains the conclusion, and Section VII concludes the paper with future directions.

II. Background and Related Work

In recent years, extensive research has been conducted on enhancing safety-critical systems like AFSS. AFSS comprises various elements, including valves, nozzles, and alarm systems, which must work seamlessly to ensure rapid and effective response to fire incidents. However, the system's reliability can be influenced by the limitations of its components. To address this issue, strategically adding backup components may help mitigate the risk of system failure and enhance overall reliability. Such backup components must also be integrated without introducing unintended behaviors and vulnerabilities.

In [3], the authors have investigated the safety of a drone system, another safety-critical system, by employing Fault Tree Analysis (FTA) and the Temporal Logic of Actions (TLA+) tool. They focused on potential failures and used formal methods to ensure system correctness.

In [4], the authors tackled the challenge of limited information on the effectiveness of fire safety systems, particularly sprinklers. This paper reviews available information on the effectiveness of sprinklers in two approaches: component-based (fault-tree) and system-based (incident data). The authors recommend including considerations for uncertainty and suggest a hybrid system/component approach for sprinkler systems.

In [5], the authors delved into a case study conducted at Rolls-Royce and Associates Limited (RRA) from February 1995 to November 1996, where the cost of owning personal computers (PCs) was investigated. The authors assessed the financial implications of PC ownership in a corporate environment. The costs were calculated based on the costs of replacing parts and the costs resulting from the unavailability of PCs due to failure. It provided valuable insight into the economic aspect of maintaining and operating complex systems.

In [6], the authors explored the application of FTA and Bayes networks for reliability estimation. They introduced the use of Bayes networks, a dynamic method for updating information about the probable failure of system components based on component data. They employed both FTA and Bayes networks for estimating the reliability of an automatic Environmental Detection and Fire Extinguisher System with a water sprinkler system and compared the results. MATLAB and Microsoft Bayes Network Software were utilized for the same. The findings revealed reduced reliability of the automatic water sprinkler system with the Bayes network due to a diesel generator acting as a standby member in case of power failure.

In [7], the authors addressed the limitations of FTA, such as its inability to account for linguistic variables and uncertainties. To overcome these, they proposed a fuzzy approach to assess the failure rates. Fuzzy probabilities enable one to represent the probability of failure for each basic event and reduce uncertainty. The authors highlight the importance of considering linguistic variables and uncertainties in reliability assessments.

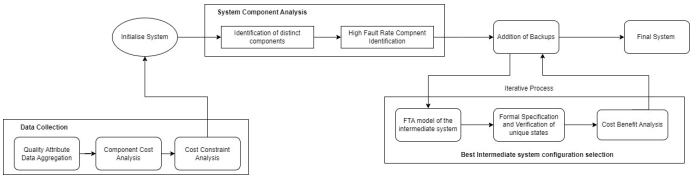

Fig. 1: Methodology

In [8], the authors investigated enhancing reliability and availability through redundancy at the level of entire machines rather than individual components. The authors further delved into the cost implications and relationship between cost and system failures of digital computers. They discussed different scenarios and penalty costs for each of them.

In [9], the authors examined the Reliability-Redundancy Allocation Problem (RRAP), focusing on imperfect fault coverage, a scenario often encountered in real-world systems. The RRAP is a challenging optimization problem that aims to allocate redundant components to a system to maximize its reliability under resource constraints. The authors introduced two fault coverage models: the Imperfect Fault Coverage Model (IFCM) and the Irrelevance Coverage Model (ICM). They emphasized that an excess of redundancy can decrease system reliability when fault coverage is imperfect. The study demonstrated that the optimal design of a system with imperfect fault coverage is different from the optimal design of a system with perfect fault coverage and that the Irrelevance Coverage Model (ICM) is a more realistic and accurate model of imperfect fault coverage than the Imperfect Fault Coverage Model (IFCM).

III. Methodology

A. Data collection

The data collection process in this paper involves two key studies. In 2011, Maximovic conducted a study to determine the data necessary for assessing the reliability of a water sprinkler system that focused on identifying failures, their underlying causes, and the limitations of data collection. Furthermore, a 2014 report titled "System Safety Engineering and Risk Assessment: A Practical Approach" by Bahr delved into an analysis of system effectiveness, including the automatic water sprinkler system, using fault tree analysis and data on failure rates, failure probabilities, and component reliability. The probability of failure for each component is detailed in Table 2.

The costs of the components are hard to find in scientific literature. Hence we have made an attempt to aggregate and collect the component costs of all the required components for various sources.

The costs are mainly based on the study carried out by the U.S. Department of Commerce Office of Applied Economics National Institute of Standards and Technology titled "Benefit-Cost Analysis of Residential Fire Sprinkler Systems".

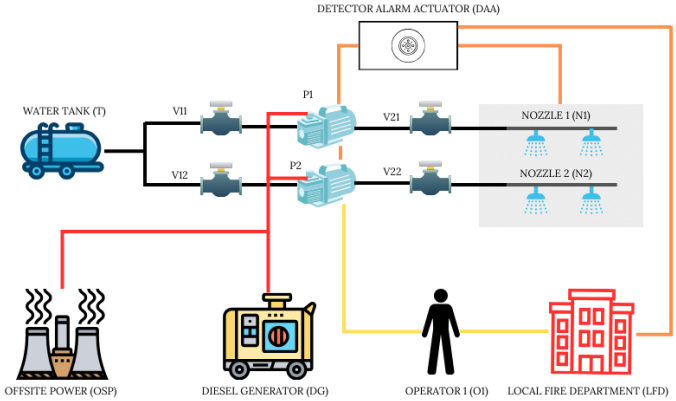

Fig. 2: Automatic Fire Sprinkler System (AFSS)

B. FTA of failure of the AFSS

An AFSS consists of several components, such as a water tank, a valve, nozzles, pumps, a heat detector, and a fire alarm panel.

1) System Introduction: In the assumed AFSS, the extinguishment of the fire majorly depends on the working of three components which are nozzle 1(N1), nozzle 2(N2) and the arrival of the Local Fire Department(LFD). Each nozzle N1 and N2 can independently manage to extinguish fire in their local areas respectively and finally the Local Fire Department(LFD) is called which extinguishes the fire of the entire area.

The nozzles N1 and N2 are automatically activated by the Detector Alarm Actuator(DAA) which sends its signal to pumps P1 and P2. The nozzles get their water supply from valves V21 and V22 respectively which in turn get their supply from pumps P1 and P2. The pumps receive power supply from an Offsite power(OSP) and in case of a power outage, a local diesel generator(DG) is able to provide power supply to the pumps, thus ensuring a constant water supply to the valves V21 and V22. The pumps P1 and P2 get their water supply from the valves V11 and V12 respectively. A water tank is installed which provides water supply to the valves V11 and V12.

The Local Fire Department(LFD) is called either by the operator(O1) or by the Detector Alarm Actuator(DAA). The Detector Alarm Actuator (DAA) is equipped with multiple batteries, charged by an external power supply, ensuring the system remains operational even if AC power is lost.

Manual valves for both pumps are normally open but can be closed during repairs. The critical components, such as the combustion system and the generator, are located outside the main body and are protected from internal fires. [4]

2) Fault Tree Analysis: We have considered the failure to extinguish the fire as the top event for the FTA. The top event occurs if any one of the nozzles (N1, N2) fails to work or the Local Fire department (LFD) fails to respond. These events that cause the top event to occur are known as intermediate events. We continue the deductive approach till the basic events. For a nozzle to get activated, the Detector Alarm Actuator (DAA) detects the fire, and the signal is sent to the pumps (P1, P2). Water from tank T enters pumps P1 and P2 through valves V11 and V12, respectively, which are then pumped into the nozzles (N1, N2) by another set of valves V21 and V22.

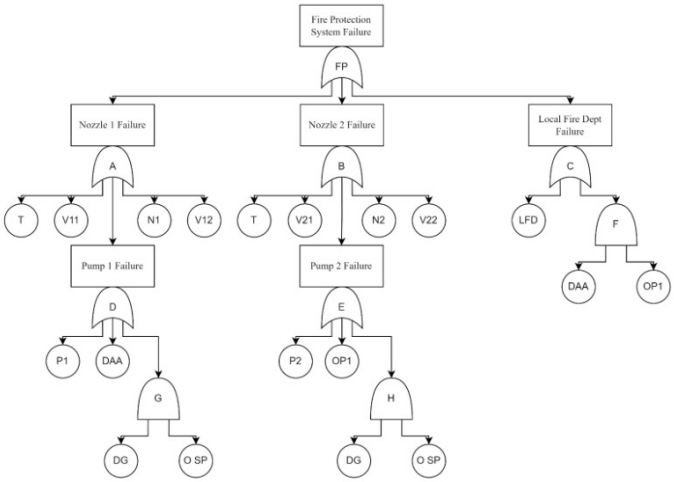

Fig. 3: AFSS of Base System

TABLE I: Abbreviations of Components

Abbreviation	Meaning
OSP	Offsite Power
DG	Diesel Generator
DAA	Detector Alarm Actuator
P1, P2	Pump 1, Pump 2
OP1	Operator 1
T	Water Tank
V11, V12, V21, V22	Valve 1, Valve 2, Valve 3, Valve 4
N1, N2	Nozzle 1, Nozzle 2
LFD	Local Fire Department

If any of the components, T, V11, P1, V21, and N1, fail, it would cause the failure of the entire Nozzle 1 subsystem. Similarly, if any of the components, T, V21, P2, V22, and N2, fail, the entire Nozzle 2 subsystem fails. The pumps P1 and P2 fail if the pumps themselves fail, the valves V11 and V12 fail, the DAA fails to send the signal to the pumps, or both the Diesel generator(DG) and the offsite power systems fail simultaneously.

For the Local fire department (LFD) to fail, there must be a failure in response to the call by the operator (OP1) based on the DAA signal or a fault in either the DAA itself or a human error by the operator.

According to the description, the fault tree of the system is shown in Figure 1. The fault tree was drawn with the help of draw.io [1] and analyzed using SHARPE tool[2].

C. Adding Redundancy to the System

To strategically add redundancy to the system, we first identify the system with high fault rates. Components susceptible to frequent failures are prime candidates for redundancy.

[1]draw.io, [Online]. Available: https://app.diagrams.net/.
[2]SHARPE, [Online]. Available: https://sharpe.pratt.duke.edu/

```
MODULE FireAlarmSystem

EXTENDS TLC

VARIABLES Pump1Fault, Valve1Fault, Pump2Fault, Valve2Fault,
OffSightPowerFault, DieselGenerator1Fault

Initialize the system with all components in a working state, and no fire detected
Init ≜
    ∧ Pump1Fault = FALSE ∧ Valve1Fault = FALSE
    ∧ Pump2Fault = FALSE ∧ Valve2Fault = FALSE
    ∧ OffSightPowerFault = FALSE ∧ DieselGenerator1Fault = FALSE

PowerFailure ≜
    ∨ OffSightPowerFault' ∈ {TRUE, FALSE}
    ∧ DieselGenerator1Fault' ∈ {TRUE, FALSE}

Pump1Failure ≜
    ∧ Pump1Fault' ∈ {TRUE, FALSE}
    ∧ PowerFailure

Valve1Failure ≜
    ∧ Valve1Fault' ∈ {TRUE, FALSE}

Pump2Failure ≜
    ∧ Pump2Fault' ∈ {TRUE, FALSE}
    ∧ PowerFailure

Valve2Failure ≜
    ∧ Valve2Fault' ∈ {TRUE, FALSE}

Nozzle1Failure ≜
    ∧ Pump1Failure ∧ Valve1Failure

Nozzle2Failure ≜
    ∧ Pump2Failure
    ∧ Valve2Failure

Next ≜
   ∧ Nozzle1Failure ∧ Nozzle2Failure

Vars ≜ ⟨Pump1Fault, Valve1Fault, Pump2Fault, Valve2Fault,
        OffSightPowerFault, DieselGenerator1Fault⟩

Spec ≜
    ∧ Init
    ∧ □[Next]_Vars
```

Fig. 4: TLA+ specification of base AFSS

The system's overall reliability is substantially improved by addressing the components most likely to fail. In conjunction with fault rates, assessing redundancy costs is also essential. The economic aspect of redundancy is evaluated to ensure cost-effectiveness. From the above analysis, we propose two hypotheses to help decide which component backups must be added.

1) Components susceptible to frequent failures (components with high failure rate) are prime candidates for redundancy
2) To ensure the greatest increase in reliability for the given cost, components that are cheaper to install backups for must be added first

To encapsulate both factors mathematically, we formulate a Redundancy Benefit (RB) term that balances the component's fault rate and the cost of adding redundancy. We assume a linear relation between Redundancy Benefit (RB) and a component's fault rate and an inverse relation between Redundancy Benefit (RB) and the cost of the component. Hence, the Redundancy Benefit (RB) is defined as the ratio of the component's fault rate (F) to the cost of introducing redundancy (C) given in equation (1), providing a quantitative measure of the potential benefit of adding redundancy to a specific component.

$$\text{Redundancy Benefit (RB)} = \frac{\text{Fault Rate (F)}}{\text{Cost (C)}} \tag{1}$$

Components are ranked based on their Redundancy Benefit (RB) values. Components with higher Redundancy Benefit (RB) values indicate a higher priority for redundancy. Components with the highest Redundancy Benefit (RB) values are top candidates for redundancy.

In addition to RB, the system architecture itself plays a role in deciding the optimum candidate component for adding backups. Suppose a system function can be carried out by two or more components, i.e. if they are connected with an 'AND' gate in the fault tree, then there is already some redundancy in that system, and adding backups to those components will have minimal effect in increasing the reliability of the system. In contrast, adding backups to the components connected with an "OR" gate would make the SCS more reliable.

Deciding the number of different components in which redundancy is added is up to the system designer. If the system designer chooses to add redundancy in only one component, the number of backups that can be installed is simply the budget assigned to the project divided by the cost of the component. However, the calculation becomes more complex if the designer chooses to add backups to two or more different components. In this case, we can approach this problem by taking inspiration from indifference curves and budget lines.

Indifference Curves (IC): In the context of redundancy, indifference curves represent combinations of backup installations across different components that yield an equivalent increase in system reliability. These curves essentially map out the trade-off between redundancy in one component versus another while maintaining the same level of reliability enhancement.

Budget Line: The budget line outlines the project's financial constraints, indicating the combinations of backups for each component that can be afforded within the designated budget. It is a critical tool for the system designer to ensure that the chosen redundancy strategy aligns with economic feasibility.

The optimal solution lies at the point where the indifference curve intersects with the budget line. At this intersection, the system designer achieves maximum reliability improvement across multiple components while staying within budget constraints. It signifies a balanced allocation of resources to enhance system robustness effectively.

The system designer can mathematically model the decision-making process by formulating equations representing the indifference curves for each component. Simultaneously, the budget line equation incorporates the cost constraints. Solving these equations simultaneously identifies the point of intersection, providing the system designer with the ideal distribution of redundancy across different components.

In the case where there are only two components that are chosen for analysis, the curve would be in two dimensions. However, the same concept can be extended to higher dimensions when analyzing more than two components.

Redundancy in the system can be added in parallel or series. In parallel redundancy, redundant components operate simultaneously, ensuring uninterrupted system reliability. This architecture is suitable for high-fault-rate components where continuous operation is critical. Series redundancy involves a sequential deployment of redundant components. It is an efficient approach for components that can be bypassed in the event of failure. For components with lower RB values or higher redundancy costs, series redundancy offers an economically viable solution. However, this will not affect our analysis of adding redundancy as in the Fault Tree. In both cases, the backups will be connected by an 'AND' gate.

D. TLA+ specification of the system with added redundancy

We use TLA+ to understand and verify the underlying intricacies of the system by understanding the expected outcomes of the system. We have encoded the Fault Tree of the system with the added backups into the TLA+ specification language. This encoding forms the basis for thorough state-space exploration, allowing us to rigorously evaluate the system's behavior. The specification aims to identify errors and test the system rigorously using the TLC model checker. All basic events in the Fault Tree are declared as variables, and the logic gates are represented by boolean operators. Each event is represented as a boolean variable whose value can be True or False. We operate with two primary states- the initial and the next. The basic events form the initial states, whereas the next state shows the relation between the intermediate events and the top events using boolean operators[3]. This specification helps ensure our system's integrity, reliability, and correctness.

E. TLC Model Checker

Once the TLA+ specification of our system is successfully parsed, the next critical step is to subject it to rigorous verification using the TLC (Temporal Logic Checker) model checker, a built-in tool within TLA+. The initial predicate must be selected, the next-state relation behavior must be defined, and the "deadlock" option must be unchecked to thoroughly explore the system's behavior. Once this is done, the TLC model checker systematically parses and evaluates all states as per the criteria set in the specification. If the specification lacks errors, the TLC model checker will successfully generate distinguished states for the initial and next states. The generation of these distinguished states and the subsequent completion of the state-space exploration serve as compelling evidence of the correctness of the SCS. It proves that the system adheres to the specified logic, behaves as intended, and is free from critical errors that could compromise its reliability.

IV. Experimentation

We build an initial system that contains the original components, as shown in the diagram.

[3]Based on the study carried out by the U.S. Department of Commerce Office of Applied Economics National Institute of Standards and Technology titled "Benefit- Cost Analysis of Residential Fire Sprinkler Systems

TABLE II: Reliability, Costs, and Redundancy Benefit (scaled)

System	λ	MTTF	Cost [3]	Redundancy Benefit
OSP	0.00011	9090.9	\$10,000	13
DG	0.055006	18.18	\$3,000	21968
DAA	0.0001	10,000	\$1,000	120
P1, P2	0.017001	58.82	\$1,000	20408
OP1	0.01	100	\$500	24009
T	0.00001	100,000	\$12,000	1
V11, V12	0.0042	238.09	\$320	15726
V21, V22	0.0042	238.09	\$320	15726
N1, N2	0.00001	100,000	\$5	2400
LFD	0.0001	10,000	-	-

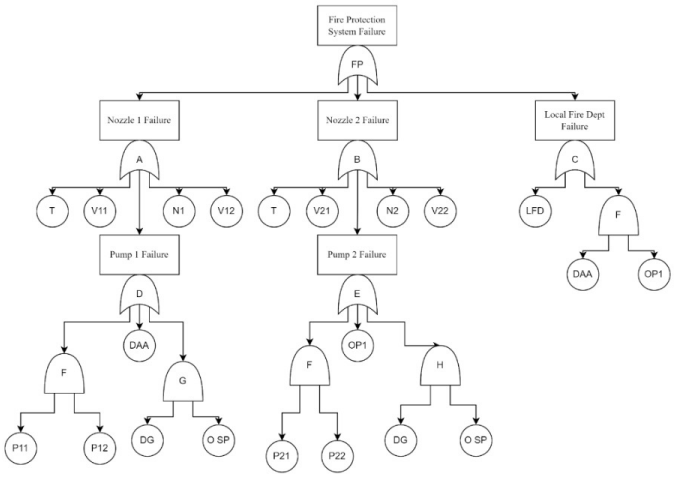

Fig. 5: Base + Backup Pumps Fault Tree.

The various components and their fault rates are mentioned above in Table 2. The redundancy benefit is calculated appropriately using the defined formula. The RB values in the table are scaled and normalized by dividing each of them by the lowest value among them all to find the relative values.

We assume a constraint budget of \$3000 available for adding redundancy.

Following our methodology, we identify two potential components with high RB to add redundancy. They are:

1) The Pumps
2) The Diesel Generator

We now construct an intermediate system with one component addition at a time. Following are the Fault Trees and TLA+ Spec of the two intermediate systems.

1) Base + Backup Pumps
   Two additional pumps are added, P12 and P22, to the initial P11 and P21 in parallel to introduce redundancy. The fault tree is built accordingly. Based on the fault tree, the TLA+ spec is created. Two additional faults, namely Pump12Fault and Pump22Fault, are added. The other components are unchanged to isolate the effect of adding pumps.
2) Base + Backup Generators
   In this intermediate system, one additional diesel generator DG2 is added in parallel to introduce redundancy.

MODULE *FireAlarmSystem*

EXTENDS *TLC*

VARIABLES *Pump11Fault*, *Pump12Fault*, *Valve11Fault*, *Valve12Fault*, *Pump21Fault*, *Pump22Fault*, *Valve21Fault*, *Valve22Fault*, *OffSightPowerFault*, *DieselGenerator1Fault*, *TankFault*

Initialize the system with all components in a working state, and no fire detected

Init $\triangleq$
$\wedge$ *Pump11Fault* = FALSE $\wedge$ *Pump12Fault* = FALSE $\wedge$ *Valve11Fault* = FALSE
$\wedge$ *Valve12Fault* = FALSE $\wedge$ *Pump21Fault* = FALSE $\wedge$ *Pump22Fault* = FALSE
$\wedge$ *Valve21Fault* = FALSE $\wedge$ *Valve22Fault* = FALSE $\wedge$ *OffSightPowerFault* = FALSE
$\wedge$ *DieselGenerator1Fault* = FALSE $\wedge$ *TankFault* = FALSE

PowerFailure $\triangleq$
$\vee$ *OffSightPowerFault'* $\in$ {TRUE, FALSE} $\wedge$ *DieselGenerator1Fault'* $\in$ {TRUE, FALSE}

Pump1Failure $\triangleq$
$\wedge$ *Pump11Fault'* $\in$ {TRUE, FALSE} $\wedge$ *Pump12Fault'* $\in$ {TRUE, FALSE}
$\wedge$ *PowerFailure*

Valve1Failure $\triangleq$
$\wedge$ *Valve11Fault'* $\in$ {TRUE, FALSE} $\wedge$ *Valve12Fault'* $\in$ {TRUE, FALSE}

Pump2Failure $\triangleq$
$\wedge$ *Pump21Fault'* $\in$ {TRUE, FALSE} $\wedge$ *Pump22Fault'* $\in$ {TRUE, FALSE}
$\wedge$ *PowerFailure*

Valve2Failure $\triangleq$
$\wedge$ *Valve21Fault'* $\in$ {TRUE, FALSE} $\wedge$ *Valve22Fault'* $\in$ {TRUE, FALSE}

Nozzle1Failure $\triangleq$
$\wedge$ *Pump1Failure* $\wedge$ *Valve1Failure* $\wedge$ *TankFault'* $\in$ {TRUE, FALSE}

Nozzle2Failure $\triangleq$
$\wedge$ *Pump2Failure* $\wedge$ *Valve2Failure* $\wedge$ *TankFault'* $\in$ {TRUE, FALSE}

Next $\triangleq$ $\wedge$ *Nozzle1Failure* $\wedge$ *Nozzle2Failure*

Vars $\triangleq$ $\langle$*Pump11Fault*, *Pump12Fault*, *Valve11Fault*, *Valve12Fault*, *Pump21Fault*, *Pump22Fault*, *Valve21Fault*, *Valve22Fault*, *OffSightPowerFault*, *DieselGenerator1Fault*, *TankFault*$\rangle$

Spec $\triangleq$
$\wedge$ *Init*
$\wedge$ $\Box[Next]_{Vars}$

Fig. 6: TLA+ Specification of AFSS with Backup pumps

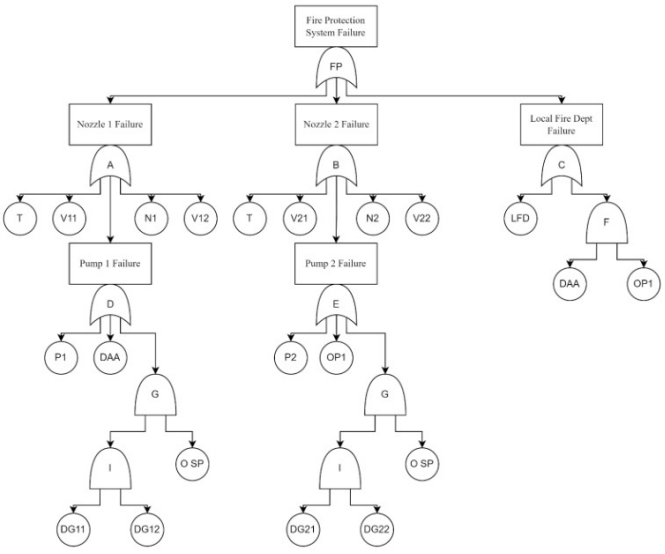

Fig. 7: Base + Backup Generators Fault Tree.

MODULE *FireAlarmSystem*

EXTENDS *TLC*

VARIABLES *Pump1Fault*, *Valve1Fault*, *Pump2Fault*, *Valve2Fault*, *OffSightPowerFault*, *DieselGenerator1Fault*, *DieselGenerator2Fault*

Initialize the system with all components in a working state, and no fire detected

Init $\triangleq$
$\wedge$ *Pump1Fault* = FALSE $\wedge$ *Valve1Fault* = FALSE
$\wedge$ *Pump2Fault* = FALSE $\wedge$ *Valve2Fault* = FALSE
$\wedge$ *OffSightPowerFault* = FALSE $\wedge$ *DieselGenerator1Fault* = FALSE
$\wedge$ *DieselGenerator2Fault* = FALSE

PowerFailure $\triangleq$
$\vee$ *OffSightPowerFault'* $\in$ {TRUE, FALSE}
$\wedge$ *DieselGenerator1Fault'* $\in$ {TRUE, FALSE}
$\wedge$ *DieselGenerator2Fault'* $\in$ {TRUE, FALSE}

Pump1Failure $\triangleq$
$\wedge$ *Pump1Fault'* $\in$ {TRUE, FALSE}
$\wedge$ *PowerFailure*

Valve1Failure $\triangleq$
$\wedge$ *Valve1Fault'* $\in$ {TRUE, FALSE}

Pump2Failure $\triangleq$
$\wedge$ *Pump2Fault'* $\in$ {TRUE, FALSE}
$\wedge$ *PowerFailure*

Valve2Failure $\triangleq$
$\wedge$ *Valve2Fault'* $\in$ {TRUE, FALSE}

Nozzle1Failure $\triangleq$ $\wedge$ *Pump1Failure* $\wedge$ *Valve1Failure*

Nozzle2Failure $\triangleq$ $\wedge$ *Pump2Failure* $\wedge$ *Valve2Failure*

Next $\triangleq$
$\wedge$ *Nozzle1Failure*
$\wedge$ *Nozzle2Failure*

Vars $\triangleq$ $\langle$*Pump1Fault*, *Valve1Fault*, *Pump2Fault*, *Valve2Fault*, *OffSightPowerFault*, *DieselGenerator1Fault*, *DieselGenerator2Fault*$\rangle$

Spec $\triangleq$
$\wedge$ *Init*
$\wedge$ $\Box[Next]_{Vars}$

Fig. 8: TLA+ Specification of AFSS with Backup Generators.

The fault tree is built accordingly. Based on the fault tree, the TLA+ spec is created. An additional variable introduced is DieselEngine2Fault.

Total reliability is a measure of the overall reliability of a system over a specified period of time. It represents the probability that a system will operate without failure during this time period.

MTTF is a measure of the expected time between the start of operation of a system and the occurrence of its first failure. It is an average time value that indicates the reliability of a system.

Mathematically, MTTF is calculated as the reciprocal of the failure rate (λ), which is the number of failures per unit of time. The formula is:

$$\text{MTTF} = \frac{1}{\lambda}$$

.

We perform a reliability analysis on the FTAs using the SHARPE tool. It simulates the behavior of the FTA over time and calculates the MTTF (Mean Time to Failure) and total system reliability.

TABLE III: Reliability values of intermediate systems

Model	MTTF	Reliability (T = 1)
Base	1.95660677e+001	9.50324501e-001
Base + Backup Generators	1.95771416e+001	9.50335090e-001
Base + Backup Pumps	3.12745535e+001	9.82632461e-001

Status

Checking FireAlarmSystem.tla / FireAlarmSystem.cfg

Success : Fingerprint collision probability: 1.1E-13

Start: 10:53:55 (Nov 1), end: 10:53:57 (Nov 1)

States

Time	Diameter	Found	Distinct	Queue
00:00:00	2	16 385	128	0

Coverage

Module	Action	Total	Distinct
FireAlarmSystem	Init	1	1
FireAlarmSystem	Next	16 384	127

Fig. 9: Statistical Report of TLC model checker for AFSS with extra diesel generator

V. Results and Discussion

TLA+ model checker results for all the intermediate systems are shown below.

A. Model with extra generator

Checking the intermediate model with the TLA+ model checker, 16,385 states were generated (383,274 s/min), 128 distinct states were found (2,994 ds/min), and 0 states were left on the queue. 16385 states generated, 128 distinct states found, 0 states left on queue. The depth of the complete state graph search is 2. The depth of 2 represents how many steps or transitions were taken from the initial state to reach the explored states.

B. Model with extra pumps

Checking the intermediate model with the TLA+ model checker, 4,194,305 states were generated (41,438,876 s/min), 2,048 distinct states were found (20,233 ds/min), and 0 states were left on the queue. The depth of the complete state graph search is 2. The depth of 2 represents how many steps or transitions were taken from the initial state to reach the explored states.

This TLA+ analysis encompassed failures at both the system and basic levels. The statistical reports from the TLC

Status

Checking FireAlarmSystem.tla / FireAlarmSystem.cfg

Success : Fingerprint collision probability: 4.7E-10

Start: 11:04:51 (Nov 1), end: 11:04:56 (Nov 1)

States

Time	Diameter	Found	Distinct	Queue
00:00:00	0	1	1	1
00:00:03	2	2 460 453	2 048	846
00:00:05	2	4 194 305	2 048	0

Coverage

Module	Action	Total	Distinct
FireAlarmSystem	Init	1	1
FireAlarmSystem	Next	4 194 304	2 047

Fig. 10: Statistical Report of TLC model checker for AFSS with extra pumps.

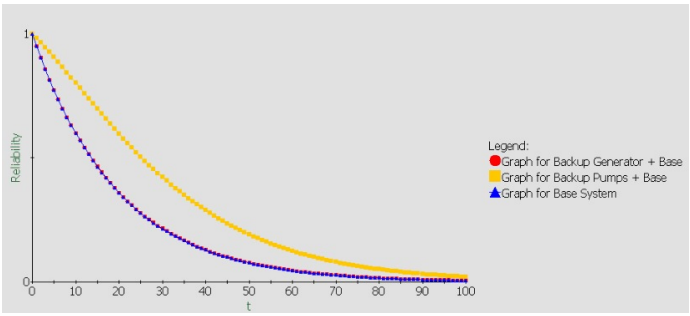

Fig. 11: Reliability Comparison for the given selective redundancy addition.

model checker suggest that the intermediate states are stable and devoid of any abnormal behaviors. They have temporal equivalence with the base system. They confirm the successful exploration of the state space, a critical aspect of model validation, as depicted in Figure 6.

The reliability comparison for the given selective redundancy addition is given in Table 3.

We can see that adding extra pumps within the budget gives us a significant increase in reliability compared to adding a generator that had a lower RB. The results of the analysis that we carried out show the following:

1) Reliability of the system increases significantly on targeting high RB components for adding redundancy.
2) The time taken to explore the states of the intermediate systems is less than testing the whole system with modifications in the TLA+ model checker.
3) The validity of intermediate systems is verified to not produce abnormal behaviors.

VI. Conclusion

Our research emphasizes the critical importance of a meticulous cost-benefit analysis when enhancing system reliability through redundancy. While the results demonstrate significant reliability improvements, it is imperative to weigh these gains against the associated costs. Although specific cost data is not provided in the present study, financial considerations play a pivotal role in the decision-making process, and a comprehensive cost-benefit analysis is essential to ensure that investments in redundancy align with the heightened reliability achieved.

Furthermore, our findings underscore the precision of resource allocation when introducing redundancy. The approach advocated in this research prioritizes allocating resources, be they financial or otherwise, to components with higher fault rates. This approach aligns with established best practices in safety-critical systems, where resource allocation is judiciously employed to fortify the most pivotal areas and guarantee reliability.

Lastly, the methodology detailed in this paper is not confined solely to the AFSS but exhibits versatility by extending its applicability to any safety-critical system. This universality

underscores the adaptability and efficacy of the approach in bolstering the reliability of systems where safety is paramount.

VII. Future Work

Our future work will encompass several key aspects aimed at advancing the application of TLA+ in the context of reliability block (RB) calculations.

A. Encoding in TLA+

A central focus of our future work involves the development of TLA+ specifications that precisely represent the RB calculation algorithms. This process will entail defining the states, transitions, and mathematical relationships inherent in the reliability assessment. The aim is to leverage the expressive power of TLA+ to accurately capture the intricacies of RB calculations.

B. Invariants and Properties

TLA+ provides a robust framework for formulating invariants and properties that capture essential characteristics of a system. In the realm of RB calculations, we plan to identify and formalize properties ensuring the correctness and reliability of the calculations. These may encompass conditions such as the conservation of reliability across components and consistency in failure rate propagation.

C. Automation and Tool Support

Our future research will delve into automating the TLA+ encoding process to enhance accessibility for practitioners. Additionally, we will explore tool support to augment the usability of TLA+ in reliability engineering. This may involve the development of tailored tools or integrations to streamline the application of TLA+ in reliability assessments.

References

[1] M. Das, B. R. Mohan, and R. M. R. Guddeti, "Formal Specification and Verification of Drone System using TLA+: A Case Study," 2022 IEEE/ACIS 23rd International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Taichung, Taiwan, 2022, pp. 156-161, doi: 10.1109/SNPD54884.2022.10051801.

[2] Spearpoint, Michael Frank, Kevin Gravestock, Neil Fleischmann, Charles. (2013). A review of sprinkler system effectiveness studies. Fire Science Reviews. 2. 10.1186/2193-0414-2-6.

[3] Bradley, Malcolm Dawson, Ray. (1998). The cost of unreliability: a case study. Journal of Quality in Maintenance Engineering. 4. 212-218. 10.1108/13552519810225209.

[4] Givehchi, Saeed Heidari, Alireza. (2018). Bayes Networks and Fault Tree Analysis Application in Reliability Estimation (Case Study: Automatic Water Sprinkler System). Environmental Energy and Economic Research. 2. 325-341. 10.22097/eeer.2019.160566.1057.

[5] Mohammadreza Bahrami, Saeed Givehchi, Full title: A novel approach for determining the reliability of sprinkler systems: A case study, Results in Engineering, Volume 17, 2023, 100843, ISSN 2590-1230, https://doi.org/10.1016/j.rineng.2022.100843. (https://www.sciencedirect.com/science/article/pii/S2590123022005138)

[6] D. E. Rosenheim and R. B. Ash, "Increasing Reliability by the Use of Redundant Machines," in IRE Transactions on Electronic Computers, vol. EC-8, no. 2, pp. 125-130, June 1959, doi: 10.1109/TEC.1959.5219513.

[7] Z. Wang, S. Zhou, D. Zhao, and J. Xiang, "Reliability-redundancy allocation problem considering imperfect fault coverage," 2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS), Hainan, China, 2021, pp. 394-403, doi: 10.1109/QRS54544.2021.00051.

[8] Forbes, J. (2023, 6th September). Generator Cost Guide. Forbes. https://www.forbes.com/home-improvement/electrical/generator-cost-guide/

[9] Trivedi, Kishor S.. "SHARPE 2002: Symbolic Hierarchical Automated Reliability and Performance Evaluator." Proceedings International Conference on Dependable Systems and Networks (2002): 544-.