



Libby Jones

2222538

Systems Engineering, Fault Tree Analysis  
ACDA 5021

University of Wales Trinity Saint David  
BENG Bachelor of Engineering Program, Ordnance, Munitions and  
Explosives (Safety)

Academic Year: 2024- 2025

1,176/1250 words  $\pm 10\%$

## **Abstract**

Fault Tree Analysis (FTA) is a foundational assessment tool that systematically breaks down undesired outcomes into their contributing failures using logic gates and probabilistic reasoning. This report applies FTA to a seemingly trivial but illustrative scenario, 'Bill's attempt to make a cup of tea', to demonstrate the method's benefits in both qualitative and quantitative risk analysis. Beginning with the construction of a fault tree, the study identifies the Top Event, successful tea preparation. Modelling its immediate causes through AND and OR gates, mapping these logical operators to set-theoretic intersections and unions for precise probability propagation. Basic-event probabilities (e.g., mains power availability, kettle integrity, cup availability) are drawn from given data and then later adjusted to reflect human-factors influences: specifically, fatigue-induced performance multipliers that reduce Bill's ability to plug in and switch on the kettle to 75% of normal and to select a cup to 90% of normal.

Quantitative calculations reveal that Bill's baseline success probability 20.3% falls to approximately 10.3% under fatigue, underscoring the critical impact of human error. The analysis highlights how minimal cut-set identification guides targeted interventions, while the integration of Performance Shaping Factors (PSFs) embeds realistic human-error rates within the fault tree. In conclusion, this case study not only confirms FTA's versatility for low-complexity tasks but also emphasises the necessity of incorporating human-factors modelling and set-theoretic workings to produce robust, actionable insights for safety and reliability enhancement.

# Table of Contents

Abstract .....ii

List of Figures .....iv

List of Tables ..... v

List of Equations.....vi

List of Abbreviations .....vii

1 Introduction to Fault Tree Analysis ..... 1

    1.1 Understanding Fault Tree Analysis ..... 2

    1.2 Expressed FTA Symbols ..... 3

2 Calculation of Probabilities ..... 4

    2.1 Calculation Approach of FTA ..... 3

3 Application of Human Factors ..... 5

    3.1 Calculation Approach of FTA, Application of Human Factors ..... 7

    3.2 Effects of Human Factors ..... 8

4 Conclusion..... 9

References ..... 10

**List of Figures**

Figure 1 Event Nomenclature for Fault Tree Calculations ..... 1

Figure 2 Fault Tree Analysis Quantitative Results Without Human Factors ..... 2

Figure 3 Fault Tree Analysis Quantitative Results With Human Factors ..... 6

**List of Tables**

Table 1 FTA Symbol Legend [3] ..... 3

Table 2 Given Probabilities of Basic Events [3] ..... 4

Table 3 - Human Factors Analysis ..... 8

**List of Equations**

Equation 1 - A1..... 3

Equation 2 - A2..... 3

Equation 3 - A..... 3

Equation 4 – B..... 3

Equation 5 - C1 ..... 3

Equation 6 - C2 ..... 4

Equation 7- C3 ..... 4

Equation 8 – C..... 4

Equation 9 - Top Event (TE)..... 4

Equation 10 -A1 Applied HF Basic Event Probabilities..... 5

Equation 11 A2 Applied HF Basic Event Probabilities..... 5

Equation 12 - A2 With Human Factors ..... 7

Equation 13 - A With Human Factors ..... 7

Equation 14 - B With Human Factors ..... 7

Equation 15 - Top Event (TE) With Human Factors ..... 7

## List of Abbreviations

|     |                           |
|-----|---------------------------|
| FTA | Fault Tree Analysis       |
| FTD | Fault Tree Diagram        |
| HF  | Human Factor              |
| PoF | Probability of Failure    |
| PoO | Probability of Occurrence |
| PoS | Probability of Success    |
| TE  | Top Event                 |

# 1 Introduction to Fault Tree Analysis

A **Fault Tree Analysis (FTA)** is a top-down, graphical technique for modelling how combinations of component failures, human errors, and external events can lead to an undesired system state (the Top Event). FTA is also commonly known as event tree analysis and is used within many industry fields. It's widely deployed in safety and reliability engineering. FTA helps practitioners understand failure logic, prioritise risk reduction efforts, and verify compliance with reliability requirements [1].

Predominantly expressed using a logic diagram, composed of various symbols, (events). The analysis of the fault tree can produce two different types of insights within their results.

**Qualitative Analysis:** Identifies minimal 'cut sets,' the smallest combinations of basic events that can cause the Top Event. This guides design improvements and the placement of barriers to enhance safety [2].

**Quantitative data:** Quantitative Analysis: Assigns frequencies or probabilities to basic event failures, allowing numerical estimation of system risk [1].

Each event within the Fault Tree Diagram (FTD), is segregated by one of two logic gates [3]:

## **OR Gates**

Represent events where the occurrence of any input event results in system failure (top event). In set theory, this is represented by the union ( $\cup$ ): if event A, event B, or both occur, failure happens.

## **AND Gates**

Represent events where all input events must occur simultaneously to cause system failure. In set theory, this is represented by the intersection ( $\cap$ ).

## **1.1 Understanding Fault Tree Analysis**

There are 4 key points to FTA which are explained below:

### **1. Identify the Top Event:**

The first step is to define the Top Event, which may represent either an undesired outcome (in fault analysis) or a desired outcome (in success analysis). For example, in an engineering context, the Top Event could be a system failure or, alternatively, the successful activation of a safety mechanism.

### **2. Break Down the Top Event:**

The Top Event is then broken down into its immediate causes using logic gates (Typically AND and OR gates to show how combinations or failures lead to the undesired event), as previously stated these gates are expressed as various symbols, these can be seen in Table 1, section 1.2.

### **3. Expand to Basic Events:**

Each contributing factor cause is further broken down into its own underlying causes until basic events are reached. These basic events represent fundamental causes such as individual human error or component failures, and this is where failure probabilities are assigned.

### **4. Analyse the Fault Tree:**

With the tree completed and probabilities assigned to the basic events, the overall likelihood of the Top Event can be calculated. This analysis also helps identify critical failure paths and areas for potential risk mitigation.

## 1.2 Expressed FTA Symbols

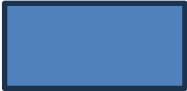
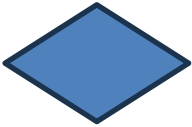
|                                                                                     |                                                                                                                  |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
|    | AND Gate – Every input must happen for a successful event                                                        |
|    | OR Gate – Any one input can cause a successful event                                                             |
|    | Fault Event – Has to be further broken down                                                                      |
|    | Basic Event – Isn't broken down further.                                                                         |
|  | Undeveloped Event – Inconsequential or doesn't have sufficient evidence or information to be further broken down |
|  | Normal Event – Expected to occur                                                                                 |

**Table 1 FTA Symbol Legend [3]**

## 2 Calculation of Probabilities

The logic diagram was created by first adding in the basic events given probabilities, these can be seen in table 2.

| Event                          | Probability |
|--------------------------------|-------------|
| Tea availability               | 0.8         |
| Coffee availability            | 0.9         |
| Chance of leaky Kettle         | 0.1         |
| Chance of water supply failure | 0.01        |
| Kettle reliability             | 0.99        |
| Plug in operation reliability  | 0.7         |
| Switch on reliability          | 0.7         |
| Mains supply failure chance    | 0.01        |
| Cup availability               | 1           |
| Cup reliability                | 0.7         |
| Milk availability              | 0.9         |
| Milk freshness                 | 0.8         |
| Sugar availability             | 0.6         |
| Sweetener Availability         | 0.9         |

**Table 2 Given Probabilities of Basic Events [3]**

These basic events were then grouped under intermediate fault events using AND and OR gates, where an AND gate signifies that all inputs must fail together, and an OR gate signifies that any one input suffices. These intersections guided how we combine event probabilities to get each branch value, this can be seen in the below Equations 1-9. Finally, multiplying the branch probabilities using the appropriate set theory calculation, gives the system's overall success probability before applying any fatigue-related adjustments.

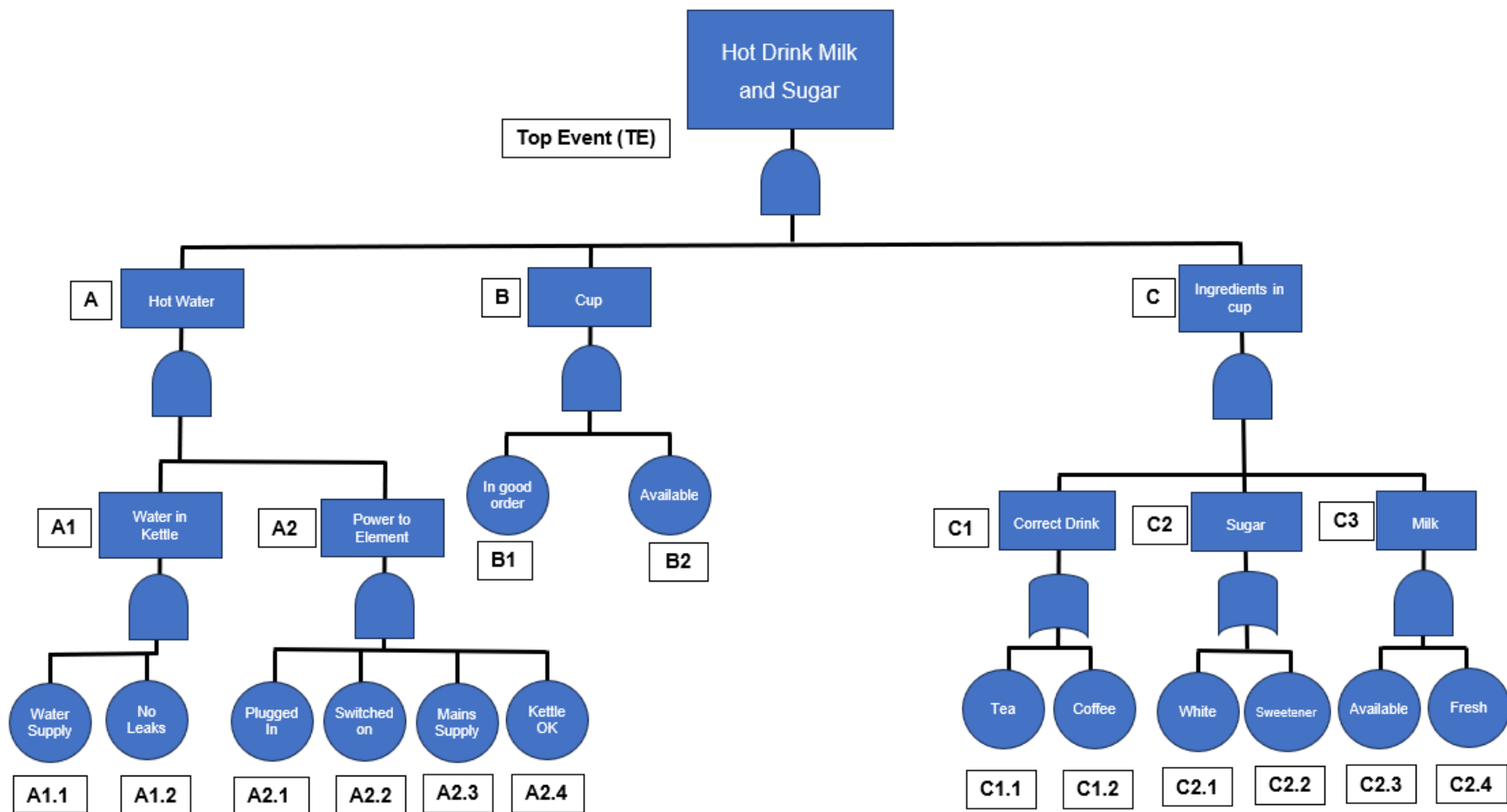


Figure 1 Event Nomenclature for Fault Tree Calculations

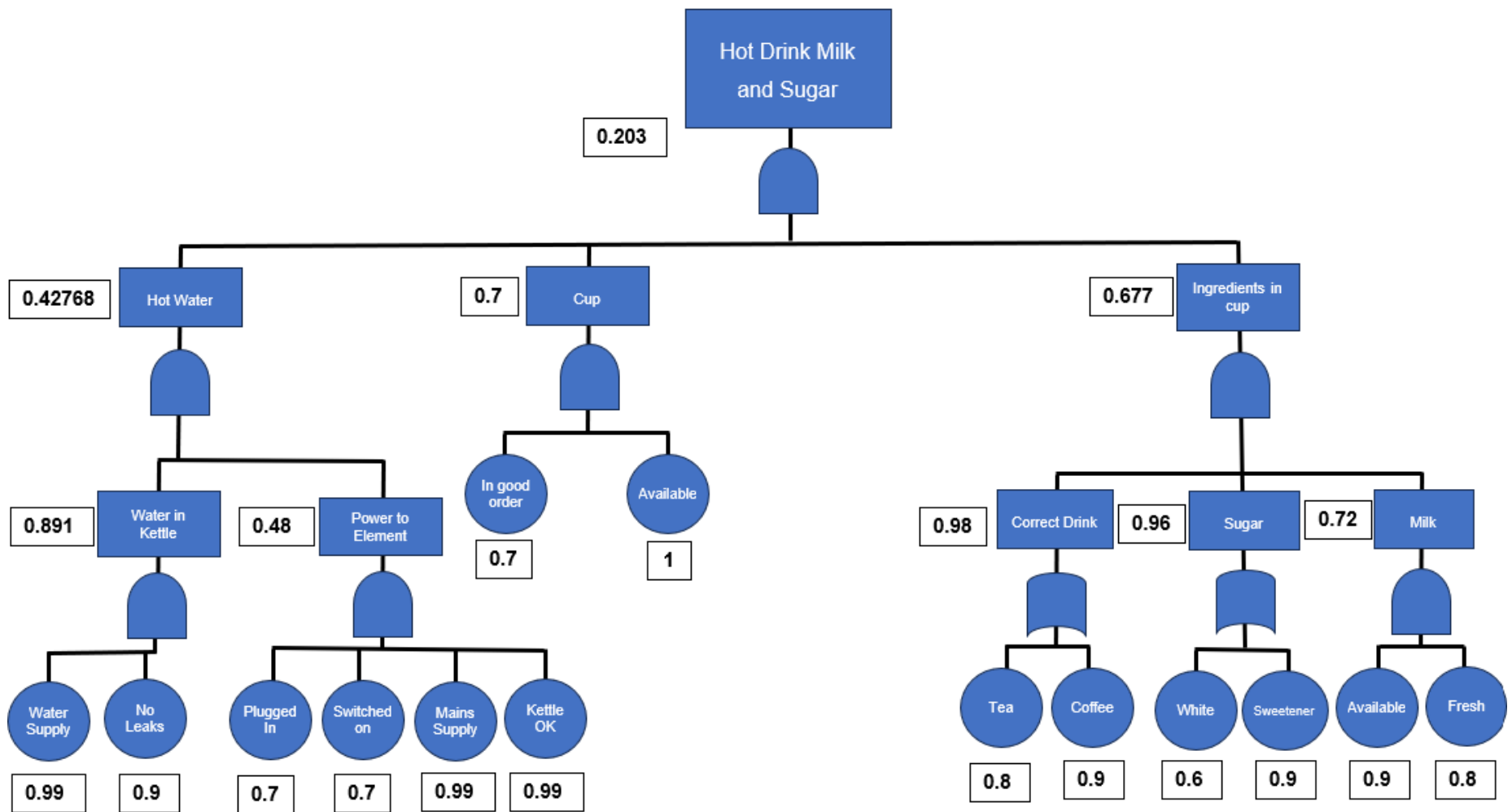


Figure 2 Fault Tree Analysis Quantitative Results Without Human Factors

## 2.1 Calculation Approach of FTA [2] [5]

### Equation 1 - A1

$$\begin{aligned}P(A1) &= P(A1.1 \cap A1.2) \\&= P(A1.1) \times P(A1.2) \\&= 0.99 \times 0.9 \\P(A1) &= 0.89\end{aligned}$$

### Equation 2 - A2

$$\begin{aligned}P(A2) &= P(A2.1 \cap A2.2 \cap A2.3 \cap A2.4) \\&= P(A2.1) \times P(A2.2) \times P(A2.3) \times P(A2.4) \\&= 0.7 \times 0.7 \times 0.99 \times 0.99 \\P(A2) &= 0.48\end{aligned}$$

### Equation 3 - A

$$\begin{aligned}P(A) &= P(A1 \cap A2) \\&= P(A1) \times P(A2) \\&= 0.89 \times 0.48 \\P(A) &= 0.43\end{aligned}$$

### Equation 4 – B

$$\begin{aligned}P(B) &= P(B1 \cap B) \\&= P(B1) \times P(B2) \\&= 0.7 \times 1 \\P(B) &= 0.7\end{aligned}$$

### Equation 5 - C1

$$\begin{aligned}P(C1) &= P(C1.1 \cup C1.2) \\&= 1 - [1 - P(C1.1)][1 - P(C1.2)] \\&= 1 - 1[1 - 0.8][1 - 0.9] \\&= 1 - [0.2][0.1] \\P(C1) &= 0.98\end{aligned}$$

**Equation 6 - C2**

$$\begin{aligned}P(C2) &= P(C2.1 \cup C2.2) \\&= 1 - [1 - P(C2.1)][1 - P(C2.2)] \\&= 1 - 1[1 - 0.6][1 - 0.9] \\&= 1 - [0.4][0.1] \\P(C2) &= 0.96\end{aligned}$$

**Equation 7- C3**

$$\begin{aligned}P(C3) &= P(C3.1 \cap C3.2) \\&= P(C3.1) \times P(C3.2) \\&= 0.9 \times 0.8 \\P(C3) &= 0.72\end{aligned}$$

**Equation 8 – C**

$$\begin{aligned}P(C) &= P(C1 \cap C2 \cap C3) \\&= P(C1) \times P(C2) \times P(C3) \\&= 0.98 \times 0.96 \times 0.72 \\P(C) &= 0.68\end{aligned}$$

**Equation 9 - Top Event (TE)**

$$\begin{aligned}P(TE) &= P(A \cap B \cap C) \\&= P(A) \times P(B) \times P(C) \\&= 0.43 \times 0.7 \times 0.68 \\P(TE) &= 0.204\end{aligned}$$

### 3 Application of Human Factors

To model the effects of human factors on the original FTD, two new basic events values were calculated under the original “Power to Element” branch as well as the “cup-selection” branch was also adjusted with one new basic event value. Creating a rippling effect to higher numerical values in the diagram such as fault events, and the top event.

Plug in Kettle and Switch on Kettle

- Under alert conditions, each of these tasks was assumed nearly perfect (Standard reliability = 0.7).
- Fatigue performance multiplier = 75%, so each task’s adjusted reliability becomes.

**Equation 10 -A1 Applied HF Basic Event Probabilities**

$$0.7 \div 100 \times 75 = 0.525$$

Cup Selection (In Good Order)

- Originally modelled as a single basic event with probability 1.0.
- Under fatigue, we apply a 90% multiplier

**Equation 11 A2 Applied HF Basic Event Probabilities**

$$1 \div 100 \times 90 = 0.9$$

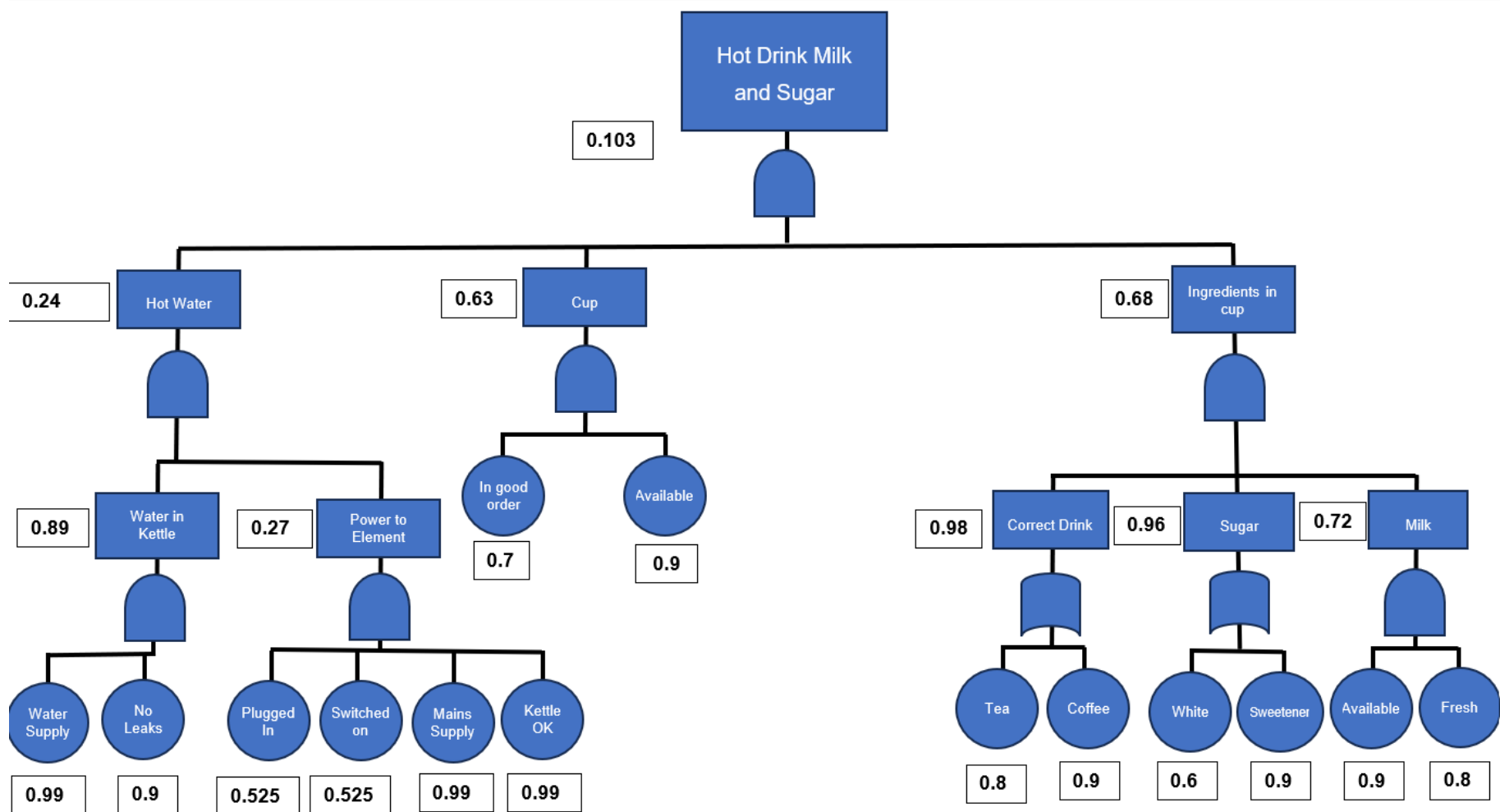


Figure 3 Fault Tree Analysis Quantitative Results With Human Factors

### 3.1 Calculation Approach of FTA, Application of Human Factors [6]

#### Equation 12 - A2 With Human Factors

$$\begin{aligned}P(A2) &= P(A2.1 \cap A2.2 \cap A2.3 \cap A2.4) \\&= P(A2.1) \times P(A2.2) \times P(A2.3) \times P(A2.4) \\&= 0.525 \times 0.525 \times 0.99 \times 0.99 \\P(A2) &= 0.27\end{aligned}$$

#### Equation 13 - A With Human Factors

$$\begin{aligned}P(A) &= P(A1 \cap A2) \\&= P(A1) \times P(A2) \\&= 0.89 \times 0.27 \\P(A) &= 0.24\end{aligned}$$

#### Equation 14 - B With Human Factors

$$\begin{aligned}P(B) &= P(B1 \cap B) \\&= P(B1) \times P(B2) \\&= 0.7 \times 0.9 \\P(B) &= 0.63\end{aligned}$$

#### Equation 15 - Top Event (TE) With Human Factors

$$\begin{aligned}P(TE) &= P(A \cap B \cap C) \\&= P(A) \times P(B) \times P(C) \\&= 0.23 \times 0.63 \times 0.68 \\P(TE) &= 0.103\end{aligned}$$

### 3.2 Effects of Human Factors

By modelling Bill's reduced ability to plug in, switch on, and select a cup, the overall chance of success falls from 20.3% to 10.3% a near 50 % reduction purely due to fatigue-induced human error. Human factors encompass the range of cognitive, physical, and organisational conditions that influence human performance and, by extension, system reliability and safety.

| Branch           | Original P | Human-Factors P |
|------------------|------------|-----------------|
| Power to Element | 0.48       | 0.27            |
| Hot Water        | 0.43       | 0.24            |
| Cup              | 0.7        | 0.63            |
| Top Event        | 0.203      | 0.103           |

**Table 3 - Human Factors Analysis**

## 4 Conclusion

This analysis has demonstrated that even simple tasks can become critical failure points when human operators are subject to fatigue and other performance-shaping factors. By integrating human reliability adjustments into the fault tree model, a nearly 50 % drop in success probability was shown. Underscoring that technology alone cannot guarantee safety or performance. As systems evolve toward greater automation, maintaining operator situational awareness, manual proficiency, and ergonomic interfaces becomes ever more vital. Ultimately, a balanced approach that combines rigorous fault tree analysis, human-centred design, targeted training, and well-defined intervention strategies will create the most robust, reliable, and resilient operations. Finally, the use of set theoretic principles, employing intersections for AND logic and unions for OR logic has provided a clear, mathematically sound foundation for combining event probabilities and revealing failure pathways, reinforcing both the transparency and robustness of the analysis. Over all Fault Tree analysis provides a well structured development of the systems failure and or success logic.

## References

- [1] A. Devasia, "Control.com," 18 June 2021. [Online]. Available: <https://control.com/technical-articles/deep-dive-into-fault-tree-analysis/>. [Accessed 12 04 2025].
- [2] "NTNU, chapter 5 Fault Tree Analysis (FTA)," [Online]. Available: <https://www.ntnu.edu/documents/624876/1277046207/SIS+book+-+chapter+05+-+Introduction+to+fault+trees/fa8ba01a-3baf-4bb8-94ed-116bf5bc6b44>. [Accessed 12 04 2025].
- [3] S. Culture, "A breif guide to fault tree analysis (FTA)," Safety Culture, 14th May 2024. [Online]. Available: <https://safetyculture.com/topics/fault-tree-analysis/>. [Accessed 12 04 2025].
- [4] D. S. L. Prof John Andrews, "An Introduction of Fault Tree Analysis," University of Nottingham, Nottingham.
- [5] D. Holley, "UWTSD," [Online]. Available: <https://moodle.uwtsd.ac.uk/course/view.php?id=12137>.
- [6] Relyence Corporation, "An In-depth Review of Fault Tree Analysis Calculation Methods," Relyence Corporation, 2024.