U.S. ARMY

DEVCOM ARMAMENTS CENTER

U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND ARMAMENTS CENTER

Proving Fuze Safety

SEP 23, 2024

Controlled by:	US Army, DEVCOM
Controlled by:	CCDC-ACM-FF, Fuze Division
CUI Category:	UNCLASSIFIED
Distribution Statement:	Distribution A: Distribution Unlimited
POC:	Stephen Redington, 520-941-0788

Proving Fuze Safety

INTRODUCTION

- Fuze safety requirements have a very long evolutionary history. Most safety requirements have been paid for with the lives of soldiers and civilians.
  - WW1 and earlier era fuzes- mostly relied on one safety mechanism and were typically inline systems. Warheads were prone to unintended functioning.
  - WW2 fuzes introduced the requirement of two independent environments for arming.
- Modern safety requirements for fuzing defined in MIL-STD-1316.
  - Base document predates 1967, Revision A circa 1969. Revision F in 2017.
  - New technology creates new safety concerns and the need for continual updating.
- Failure mechanisms become less obvious as technology and design complexity increases.

Proving Fuze Safety

INTRODUCTION

Safety and arming are primary roles performed by a fuze:

- Maintains munition safety throughout the Life Cycle Environmental Profile (stockpile-to-target sequence)
- Initiates the munition’s warhead when the target is detected

- The **purpose** of MIL STD 1316 is to establish design safety criteria for fuzes and Safety and Arming (S&A) devices that are subsystems of fuzes.
  - Establishes Design Safety Criteria for Fuzes
  - Mandatory elements of design, engineering, production and procurement of fuzes
  - Design Approval
  - **Verification**

The inadvertent arming and firing of a fuze system can result in Catastrophic material damage & injury or Death to personnel.

- Every effort must be made during the development of the munitions’ fuze safety system to achieve a high degree of safety during the lifecycle:
  - Prior to intentional initiation of the arming sequence (shipping and handling)
  - Prior to tube exit
  - Prior to safe separation

Proving Fuze Safety

METHODS FOR ENSURING SAFETY

- Safety cannot be inspected in; It must be designed in!
  - ➢ Analysis
    - – Failure Mode Effects Analysis (FMEA).
    - – Failure Mode Effects Critical Analysis (FMECA). Includes criticality, assurances and controls.
    - – Fault Tree Analysis (FTA).
      - • Probability of unintended function.
    - – Reliability Analysis.
      - • Probability of intended function.
  - ➢ Testing
    - - Developmental testing – Does it meet the design requirement?
    - - Qualification testing – Does it meet the user requirement?
  - ➢ Reviews
    - – Peer reviews.
    - – Review boards.

Proving Fuze Safety

METHODS FOR ENSURING SAFETY

➢ REVIEW BOARDS

- Responsible for compliance. Examines safety prior to and including launch.
  - Production, shipping, handling, storage, loading, launch, safe separation.
  - Each service has their own review but meet jointly when fuzes are used on common munitions. All work together to ensure user safety across all services.
    - ✓Army Fuze Safety Review Boards – AFSRB.
    - ✓Navy Fuze & Initiation Systems Technical Review Panel – FISTRP.
    - ✓Air Force Nonnuclear Munitions Safety Board (NNMSB).
    - ✓Joint Service Fuze and Ignition Systems Safety Authorities (JS-FISSA)
  - Each requires intimate knowledge of how the fuze works (no secret sauce).
- In addition, the System Safety Review Board (SSRB) is concerned with overall safety, including:
  - Overhead safety.
  - Reliability.
  - UXO.

Proving Fuze Safety

UNDERSTANDING THE SYSTEM SAFETY ISSUES

- What is the safety issue
  - Catastrophic loss of life or property.
- It is critical to understand and communicate how the system is intended to operate
  - State diagrams.
  - Logic diagrams.
  - Schematic diagrams.
  - During safe separation.
- It is critical to understand and communicate how the system can fail
  - This requires imagination
  - Is never 100% inclusive
  - Murphy's law applies, If anything can go wrong just assume it will.

Proving Fuze Safety

UNDERSTANDING THE SYSTEM

Caution 1

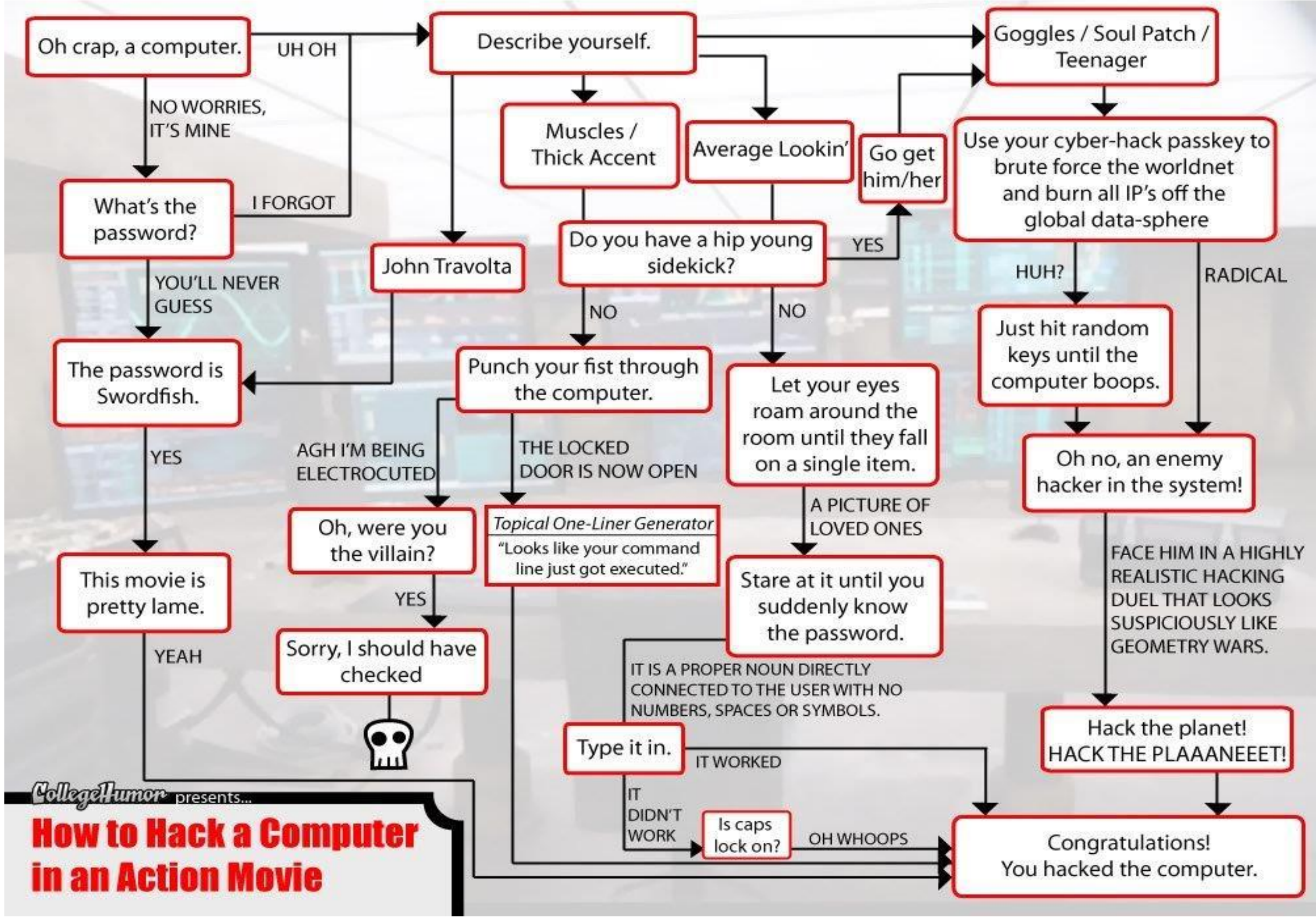
Oversimplifying a complex system

Proving Fuze Safety

UNDERSTANDING THE SYSTEM

Caution 2

Misrepresenting a Complex system

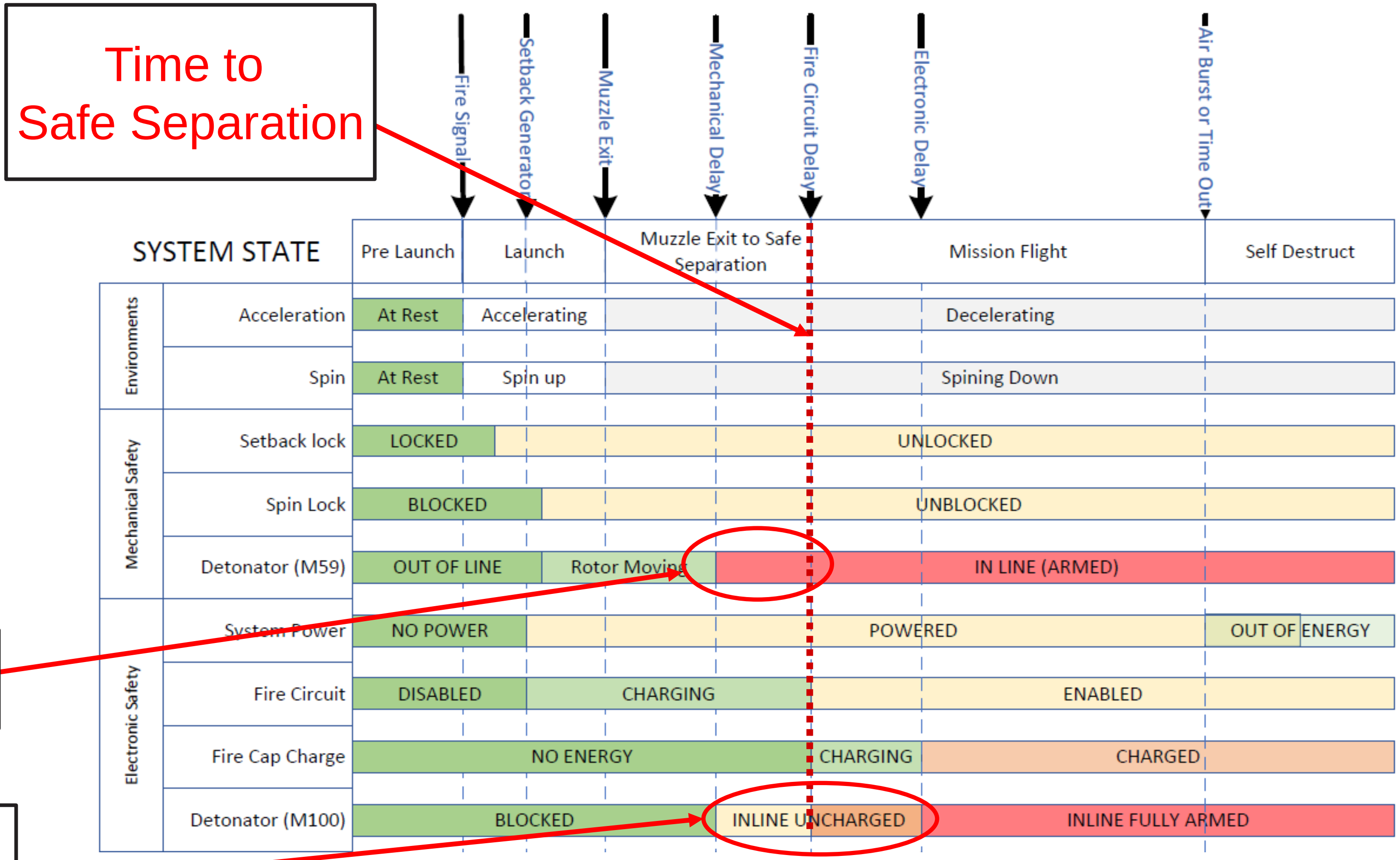


Proving Fuze Safety

UNDERSTANDING THE SYSTEM

A real example

FUZE ARMING SEQUENCE



Safety Issue

Mitigation Logic

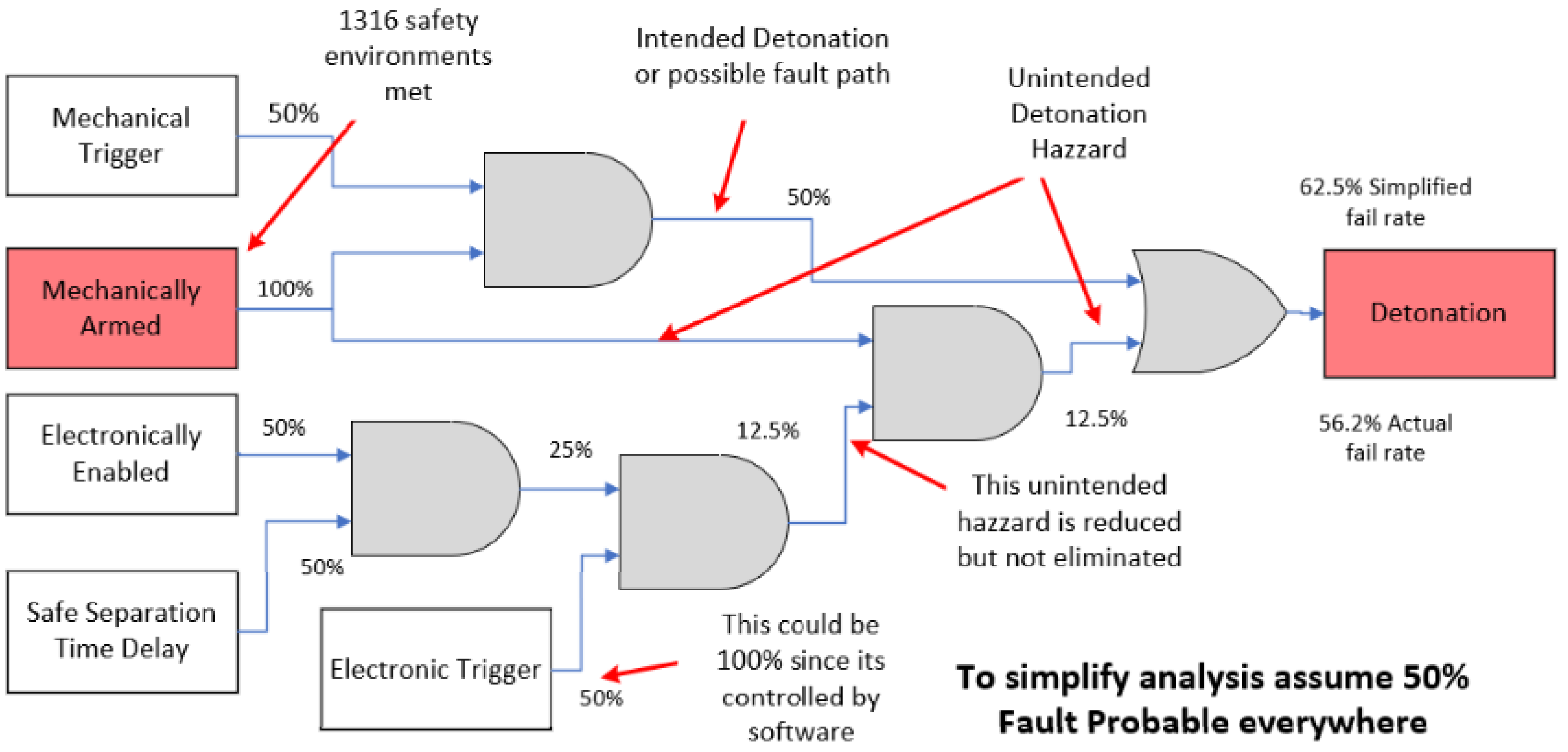
An Arming Sequence/State Diagram

Proving Fuze Safety

UNDERSTANDING THE SYSTEM

- A real Example

FUZE ARMING SEQUENCE



Arming Sequence as a Logic Diagram for FTA

Proving Fuze Safety

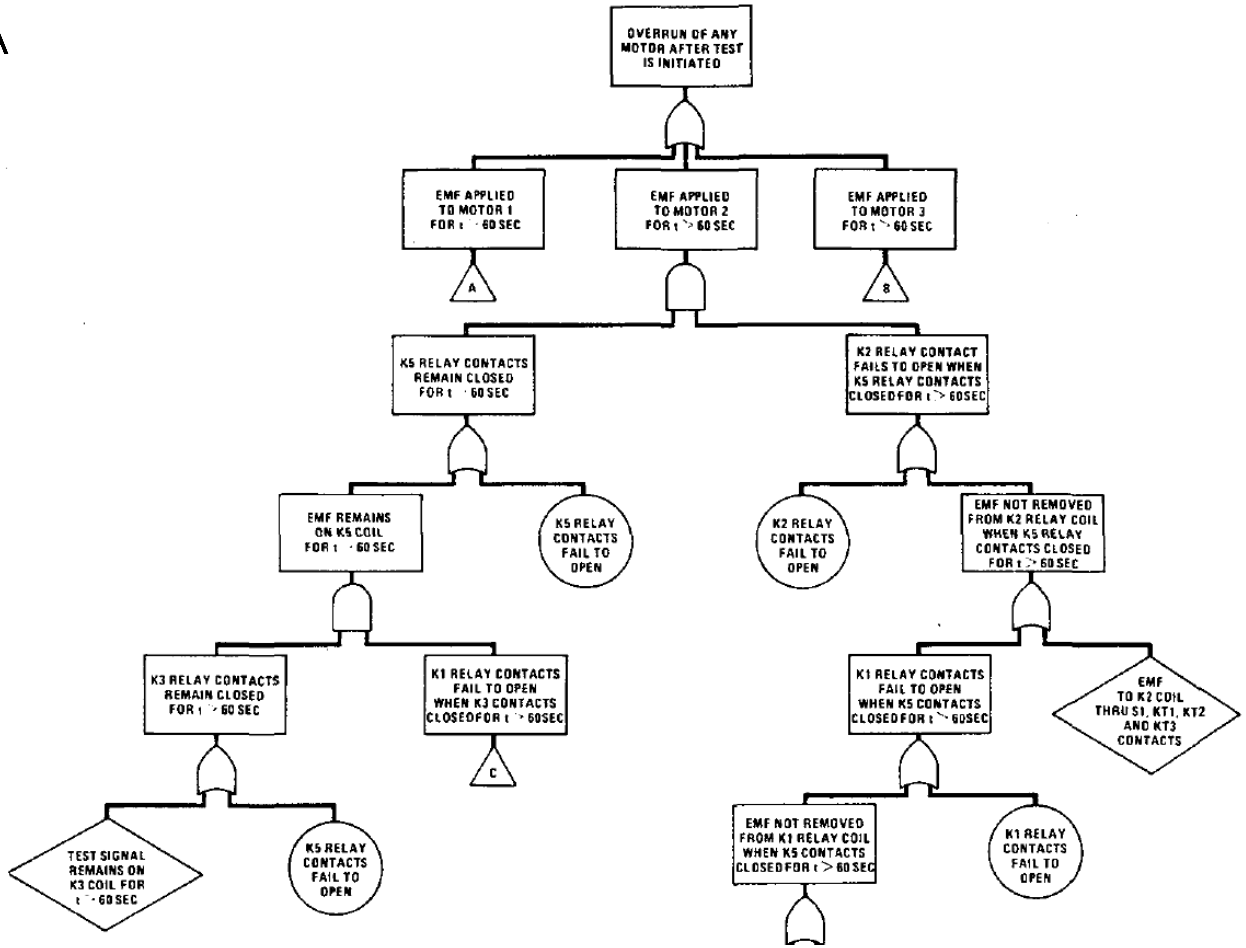
FAULT TREE ANALYSIS

- What is the probability of unintended functioning.
  - During assembly.
  - During shipping and handling.
  - During launch.
  - During safe separation.
- Not concerned with functioning as intended.
- A necessary safety document for review boards.
- Guidance for performing the FTA is not well documented in a single standard but it is a necessity for proving safety. Work is ongoing on formalizing guidance in a new JOTP (Joint Ordinance Testing Procedure) through the work of the FESWG (Fuze Engineering Standardization Working Group).
  - A logic diagram of the safety critical system is required. System operation must be clearly understood.
  - Multiple documents/requirements exist.
  - FTA calculations with probabilities greater than 100% indicate a lack of understanding.
  - FTA calculations depending on probabilities smaller than 10^{-12} also misses the point of the analysis

Proving Fuze Safety

FAULT TREE ANALYSIS

- Example FTA



Example FTA Logic Diagram from NUREG-492

Proving Fuze Safety

FAULT TREE ANALYSIS (FTA)

Requirements from MIL-STD-1316 for Launched Munitions

EVENT	SCENARIO	ACCEPTABLE PROBABLY
ARMING	Prior to Launch	1 E^{-6} (1: 1,000,000)
	Prior to Launch Tube Exit	1 E^{-4} (1: 10,000)
	Prior to Safe Separation	1 E^{-3} (1: 1,000)
FUNCTIONING	Prior to Launch	1 E^{-6} (1: 1,000,000)
	Prior to Launch Tube Exit	1 E^{-6} (1: 1,000,000)
	Prior to Safe Separation	As Low as Practical

- **Primary Intent is to demonstrate there are no single point failure modes in the design**
- **FTA should therefore be evaluated based on the FUZE DESIGN Robustness, and not weighted on production/quality assurance history (in other words, safety performance should be assured by design with less reliance on inspection)**
- **Source for component failure probability numbers: conservative engineering judgment; numerous software FTA programs and historical documents; MIL-HDBK-217F for electronic components**

Proving Fuze Safety

FAULT TREE ANALYSIS

- A Logic diagram is essential – Based on fundamental understanding of the system.
  - All functional elements can be reduced to a series of logical operations involving 'AND', 'OR', and NOT gates. (Symbols can include XOR, NAND, NOR).
  - A conservative and realistic probability of failure/fault is assigned to each component of the operation. These can be reduced with rationale on subsequent passes if needed.
  - 'AND' operations will decrease probabilities. Cascaded operation will asymptotically reduce probabilities to zero but never reach zero.

AND Probabilities simply multiply: $P = A * B$ Exact

  - 'OR' operations will increase probabilities. Cascaded operation will asymptotically increase probabilities to 100% but never exceed 100%.

OR probabilities are complicated:

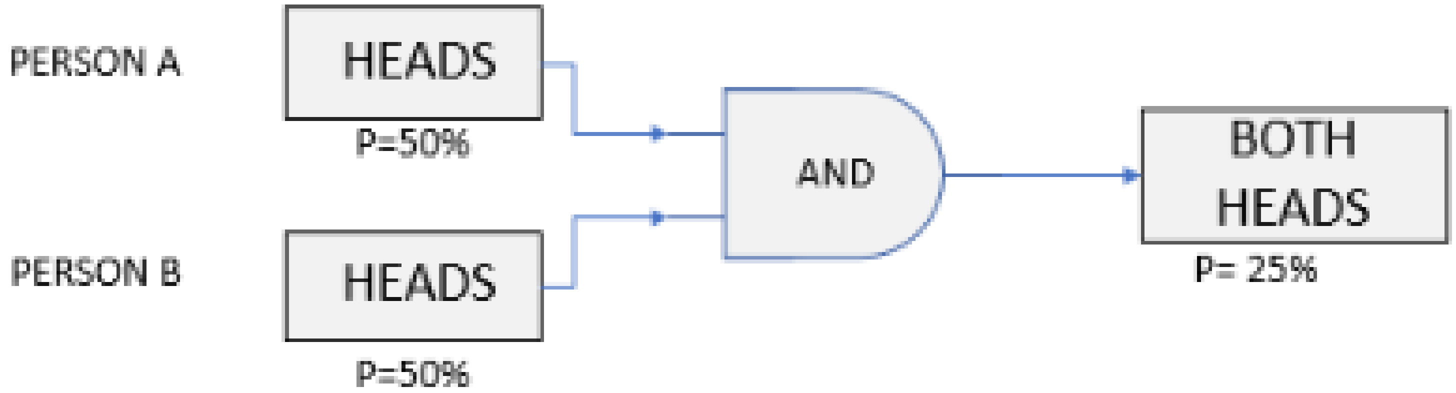
$P = (A + B) - (A * B)$ Exact

$P = A + B$ Simplified

Proving Fuze Safety

FAULT TREE ANALYSIS

- EXAMPLE1. What is the probability of two individuals getting ‘heads’ when flipping a coin?
  – As common sense would predict: The individual probabilities multiply.

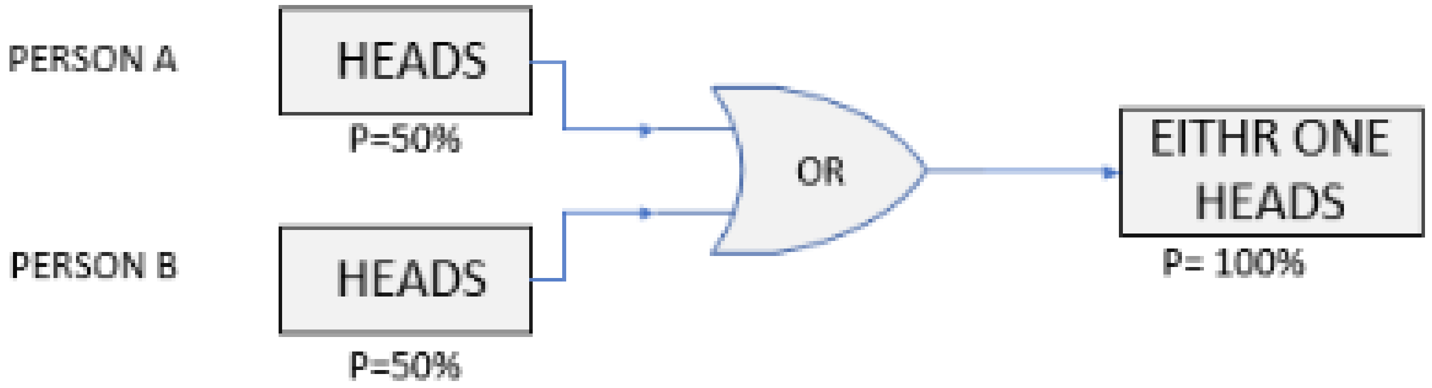


  – This makes sense! If you want to make your system safer, require more things to go wrong in parallel. i.e. Safety depends on two independent environments.

Proving Fuze Safety

FAULT TREE ANALYSIS

- EXAMPLE2. What is the probability of one individual getting 'heads' when flipping a coin?
  - If we use simplified logic.

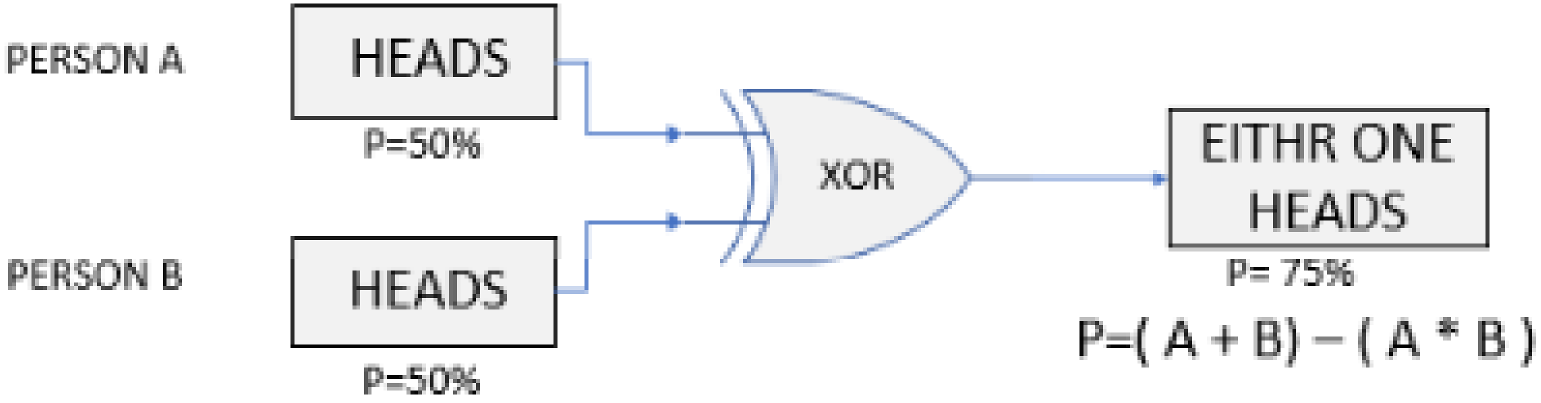


  - Hmmm… Something seems wrong here! What happens when we add a third person? 150% chance of getting heads cannot be correct!
  - This result is nonsense and damages the credibility of the analysis.

Proving Fuze Safety

FAULT TREE ANALYSIS

- EXAMPLE3. What is the probability of one individual getting ‘heads’ when flipping a coin?
  - If we use exact logic ‘OR’ becomes ‘EXCLUSIVE OR’.



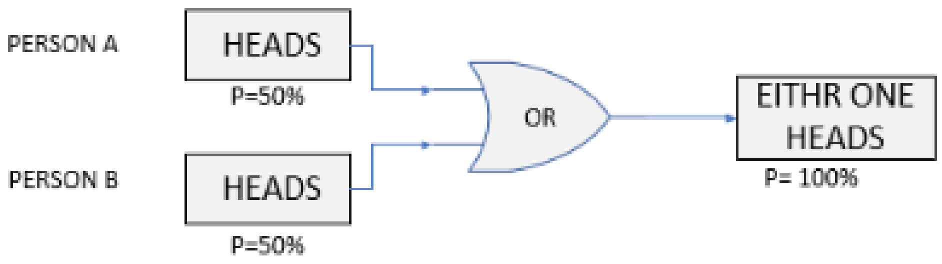
  - This works, but why?
    - ➢We want an ‘exclusive or’ condition! We need to subtract the possibility that both were heads since any one result constitutes a ‘failure’.

      i.e. The system fails when A or B fails. We do not care if both fail.

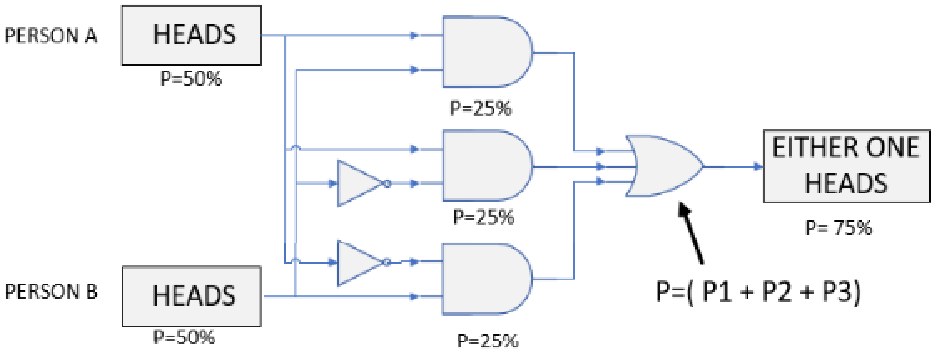
Proving Fuze Safety

FAULT TREE ANALYSIS

- When adding (OR'ing) failure mechanisms its easy to use the wrong logic!



Simplified



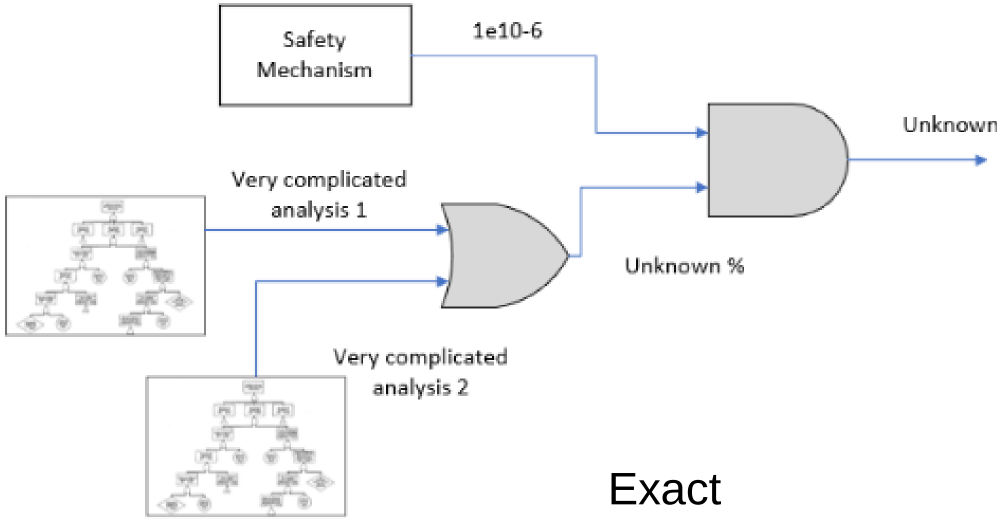
Exact

- Simplified logic only works when input probabilities are small! (i.e. probabilities less than 5% result in a .25% error / 50% probabilities result in 25% error).
  - As per AFSRB guidance: Software and microprocessor logic introduces terms on the order of 100%. This is where the conventional 'simplified' analysis falls apart. Nobody would ever intentionally design in a failure mechanism with a 50% or higher fail probability.

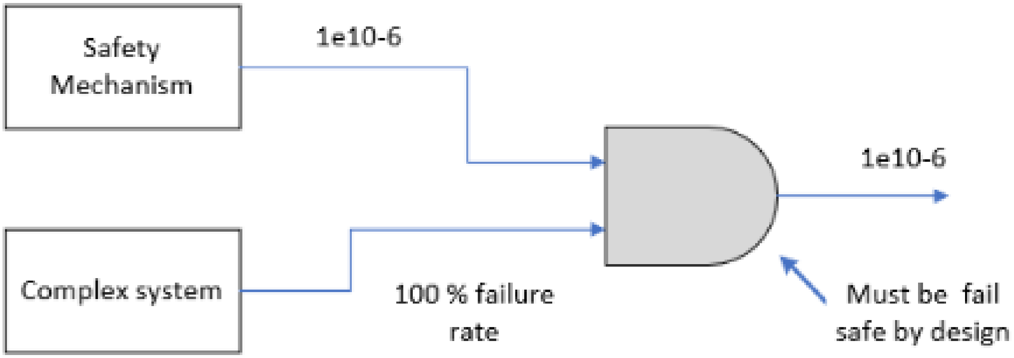
Proving Fuze Safety

PRUNING THE FAULT TREE

- Why?
  - To avoid analyzing paths that are overcomplex
- How?
  - By assuming a probability of failure of 100% we eliminate all contributing elements in this path
- When can you do this?
  - When the outcome is gated (AND’ed) out by a low probability of failure and the result meets the safety criteria. Software controlled trigger are a perfect example



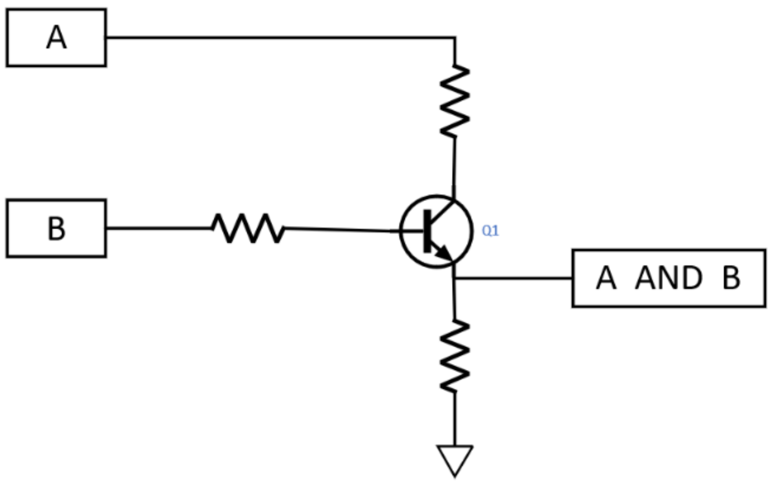
Exact



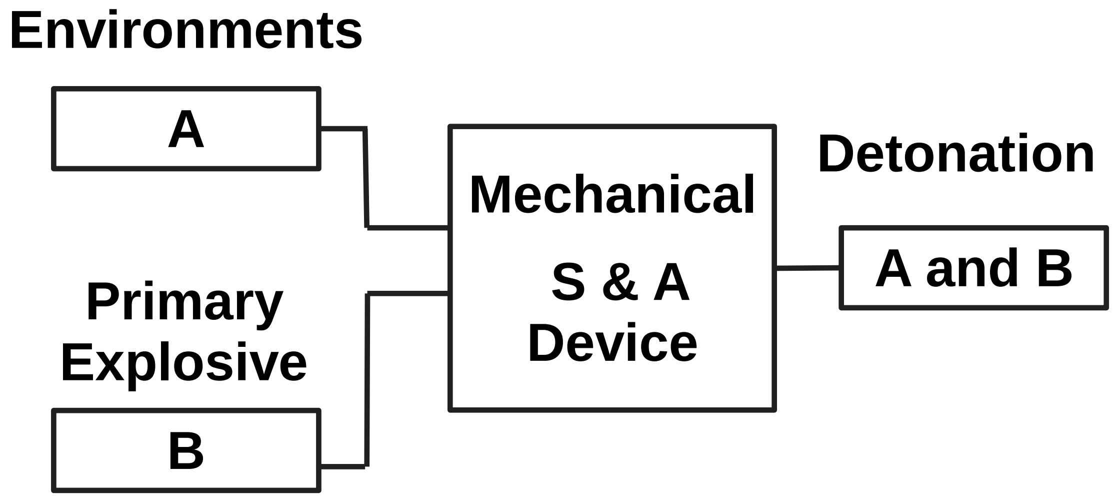
Simplified

Proving Fuze Safety

PRUNING THE FAULT TREE



Electrical And Gate



Mechanical And Gate

Fail Safe AND Gates

Proving Fuze Safety

IN GENERAL

- Fault trees are built from a logical model of the system. This includes a sequence of events (outcomes) fed by the logic or input to the system from the lowest levels.
  - – A bottom-up analysis.
- Results are dependent on assumed probabilities of fault mechanisms.
  - – Physical factors.
    - – An electronic component fails.
    - – A mechanical component breaks.
    - – Environments cause freezing / melting.
  - – Human factors.
    - – An operator installs the wrong component.
    - – An operator skips a step in assembly.
    - – Something is mislabeled.
  - – MIL-STD-882, System Safety provides guidance for root cause probabilities.

Proving Fuze Safety

YOU CAN ALWAYS EXPECT THE UNEXPECTED

- Despite rigorous analysis, testing and review, safety critical systems can manage to find new ways to fail.
  - ➢Most will involve human factors.
  - ➢All will involve mechanisms and interactions never conceived of. Examples from my 40 years of experience.
    - Example1: Early termination of STS-83 in 1997. Root cause: Technician not cutting strings with scissors as per documented instructions.
      - Fuel cell failure leads to shut down of non-critical systems.
      - Excessive moisture build up and condensation in cabin.
      - One IMU (Inertial Measurement Unit) fails causing early mission termination IAW flight safety rules (i.e. three guidance IMU's required at all times).
    - Example2: Aperiodic network outages for over 2 years. Root cause: Landscape service not reading English.
    - Example3: Certified component failures. Root cause: Marking component with 'pass'.

Proving Fuze Safety

IN CONCLUSION

- You can claim a system is 100% safe but not 100% of the time.
- In the end, safety will depend on the quality of the assumptions made in the analysis.

Proving Fuze Safety

REFERENCES

- DOD, MIL-HDBK-338B, Electronic Reliability Design Handbook, Oct 1998
- Texas A & M University, Fault Tree Analysis, Construction/Evaluation/ Application. Preston l. Parker, 1977
- DOD, MIL-STD 1316F, Fuze Design Safety Criteria, 2017
- DOD, MIL-STD-331D, Fuze and Fuze Components Environmental and Performance Tests for
- DOD, MIL-STD-882D, System Safety
- Fault Tree Handbook, NUREG-0492, 1981

QUESTIONS?

THANK YOU.

For more information feel free to contact:

Stephen Redington: stephen.h.redington.civ@army.mil

U.S. ARMY