

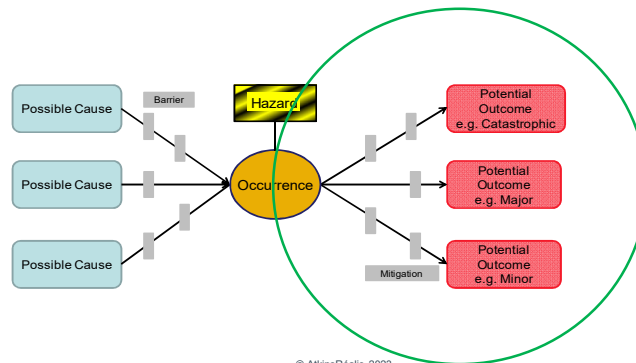
Event Tree Analysis

Learning Objectives

- To introduce event trees
- To show how event trees should be constructed
- To discuss ways in which event trees can be used in both development and operation of safety critical systems
- To show how event trees can be used in probabilistic safety calculations.

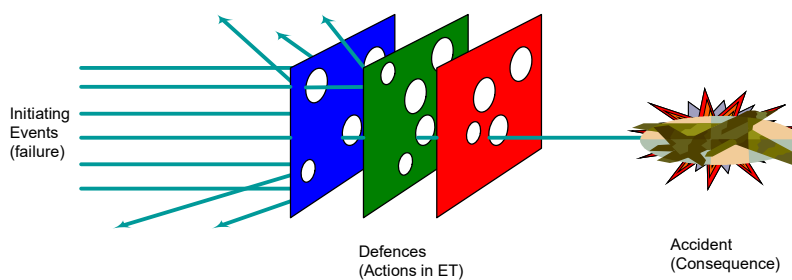
Introduction to Event Trees

- An Event Tree is a representation of possible sequences of events
- Analysis is *inductive* technique, i.e. working from an event to its possible consequences
- Event Trees allows an assessment of the ability to manage failed systems to be conducted - avert the progression to an accident.



© AtkinsRéalis 2023
AtkinsRéalis - Baseline / Référence

“Swiss cheese” model and ETA

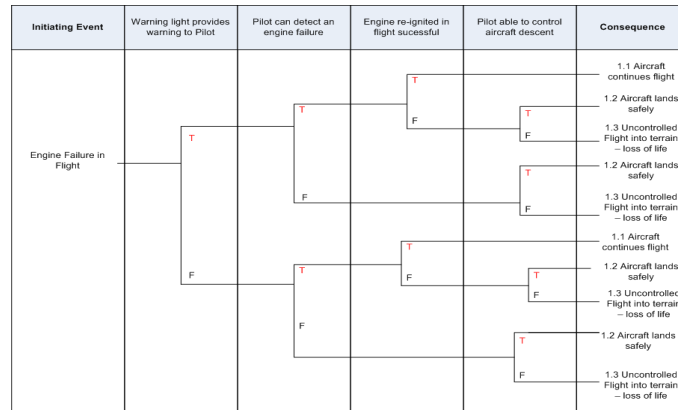


- How the accident sequence propagates through the defences depends on any interaction with the defences and how the ‘holes’ align
 - The blocking of one sequence might resulting in a branching to another sequence
- ETA explores the accident sequence to determine the full range of possible outcomes.

© AtkinsRéalis 2023
AtkinsRéalis - Baseline / Référence

Event Trees

- Starting from an **initiating event**
 - Outcomes branch off like a tree
 - All events are true/false (Boolean logic)
 - Follow the accident sequence until consequences are determined!



© AtkinsRéalis 2023
AtkinsRéalis - Baseline / Référence

Event Trees – Construction Rules

- Initiating event on left hand side
- Subsequent events as columns
 - Columns headed with a short statement of event
 - Events all phrased so **TRUE** is desired outcome
 - Phrased as binary decision (**TRUE/FALSE** or **YES/NO**)
 - simplifying assumption – EITHER something works perfectly (achieves its intent), OR it is considered to have failed
 - Normally don't include quantitative effects
 - “Automatic sprinklers extinguish fire” ✓
 - “Flow through sprinklers is more than 30% of design capacity” ✗
 - “Best” outcome are always placed on top branch
- Outcomes listed at end of each sequence
 - Final event tree illustrates the range of possible outcomes
 - “Best” outcome always end up at the top.

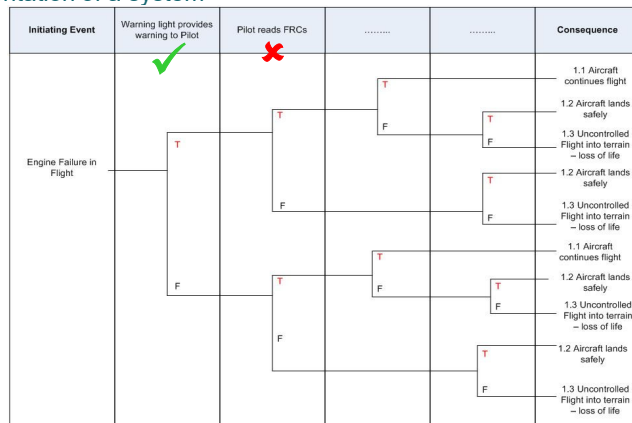
© AtkinsRéalis 2023
AtkinsRéalis - Baseline / Référence

Types of Events

- Typically 2 types of events to consider
 - Environmental Factors
 - Aspects of the working environment that are not within our control
 - Control and Mitigators
 - Planned responses to reduce accident probability or limit impact
- Groups of events to think about – the “4 M’s” (include environmental aspects)
 - Machines
 - Sensors, automatic systems, alarms, interlocks, design etc.
 - Materials
 - Fire suppression, low smoke, fire retardant, non toxic, etc.
 - Mensch
 - Human detection and intervention, Emergency Services (the human as the hero)
 - Methods
 - Procedures e.g. Post flight maintenance.

What Events to Include?

- Interested in key decisions
 - should not include too much detail otherwise tree will get too big & unwieldy
 - REMEMBER - Representation of the accident sequence, and NOT a representation of a system
- Only include columns where there is a decision
 - Don't include things which are certain or impossible



Sequences Matter!

- Events in columns are often NOT independent
 - “Successful evacuation” is very dependent on previous event of “fire alarm sounds”



- Often referred to as **System Dependencies** and **Conditional Responses**
 - System Dependencies – most systems interact with other machines or processes which may degrade levels of protection. E.g. air-conditioning failure leading to overheating
 - Conditional Responses – Success of event may be conditioned by preceding event. E.g. pilots ability to visually detect a conflict is dependant on weather conditions.

© AtkinsRéalis 2023
AtkinsRéalis - Baseline / Référence

ETA Workshop

Workshop

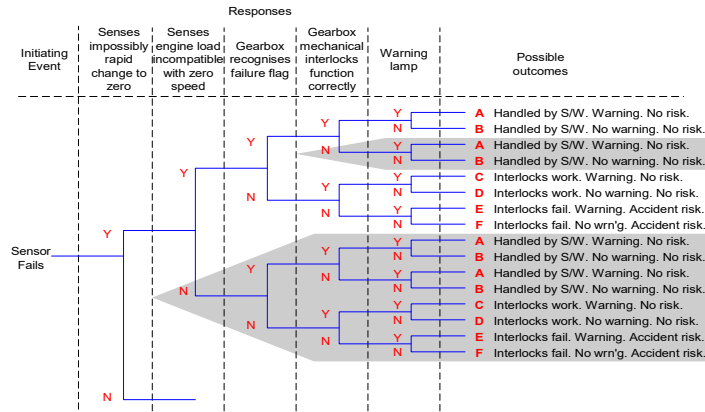
- Initiating Event:
 - Fuel Leak in Pod
- Determine what the main column headers are
 - Controls
 - Decision points
 - Aggravators
- Build the event tree
 - Remember not all branches result in subsequent branching
 - Some may pass straight through a column without branching
- Determine the Consequences

Workshop Wrap Up

- Determining column headers is tricky
 - The level of granularity determines how big the Event Tree becomes
- The only way of reaching a nil effect “safe” outcome involves detecting the leak
 - Detection is a key control
- Identifying the range of outcomes results in more consequences identified
 - Fire is the obvious consequence
 - Tanker fuel starvation and dowsing maintainer with fuel are other consequences that might not have been mitigated if they had not been identified

Managing Event Trees

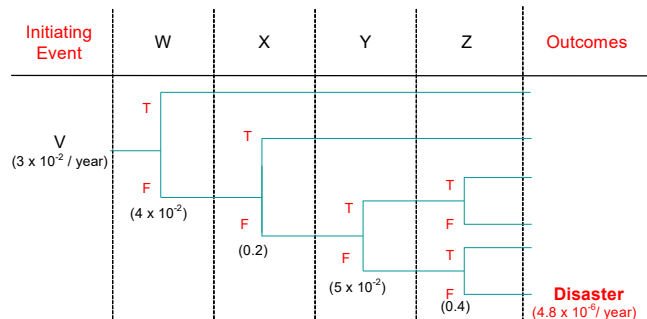
- Can 'prune' redundant branches
 - where outcomes are the same regardless of success / failure



- Sometimes useful to leave apparently redundant events in the tree
 - e.g. when calculating probabilities

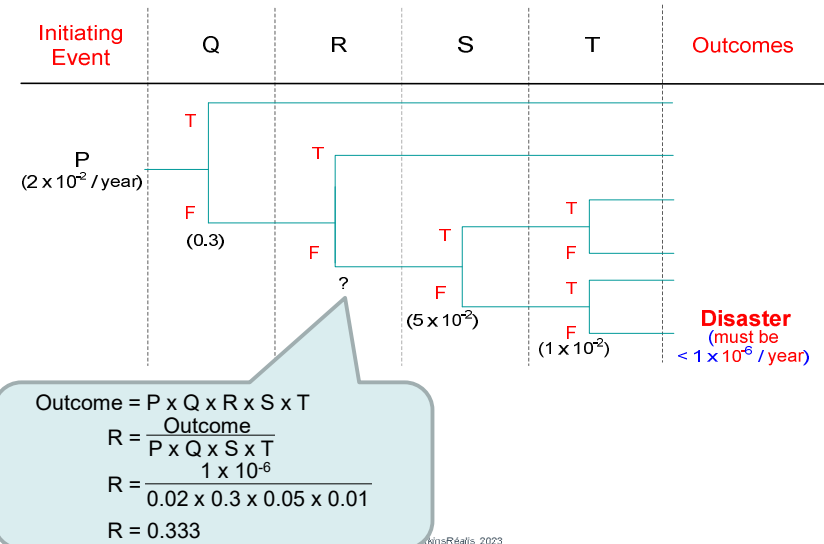
Probability Calculations

- Decision follow Boolean Logic:
 - $p(\text{success}) + p(\text{failure}) = 1$ or $p(\text{success}) = 1 - p(\text{failure})$
- All events must occur to complete the sequence, so simply multiply probabilities



- Events (columns) may not be independent, so probabilities are *per decision*, not per column

Target Setting



Event Trees – When to Use?

Most useful early in design / development of equipment or procedures

- Key (high-level) questions
 - What *could* happen?
 - Is there *sufficient* protection?
 - Are protective measures *independent*?
- Can apply probabilities to events
 - Calculate likelihood of outcomes
 - Set targets (required probability) for success of protective measures

Also useful in operation

- *IF* this changes (e.g. shut down a system for maintenance), what are new possible sequences / levels of protection / probabilities?

NOT appropriate for

- Investigating causes of a specific outcome – that is role of Fault Trees
- Accident investigation
- Detailed analysis of very complex systems – tree diagrams become intractable.

Questions to Ask

- Have event trees been constructed for the right events?
 - Obvious starting points for development of major hazards
 - Significant technical or human failures
- Are event sequences credible?
 - Appropriate events included
 - Too much / too little detail
 - Dependencies between events correctly represented
 - Outcomes identified and properly described
- How have event trees been used?
 - Justification of equipment design / procedure development
 - Source of reliability data used
 - Investigation of options.

Have the learning objectives been met?

- Why do we use Event Trees?
- When would Event Trees be used?
- How can targets be set in Event Trees?

Questions