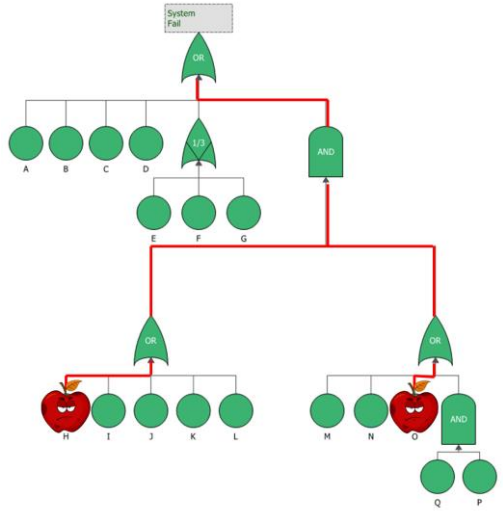
HBK Technology Days – Virtual Seminar Series

Tuesday, November 22, 2022



Fault Tree Analysis – the Critical Path! – Uncover your Unreliability Drivers

Presented by Chris Wynn-Jones and Sam Eisenberg
Reliability Application Engineer & Product Manager, HBK ReliaSoft Products

UNRESTRICTED

Fault Tree Analysis

Abstract

A Fault Tree is used to identify the critical path/s in a process, system or service. This introduction will focus on two different views, top down and bottom up.

Top Down. This view is read downwards, from undesirable events down to the lowest known fault/cause branch item. All the undesirable events that can result from your Process, System or Service, are driven by something that is no longer working correctly. Engineers use this mentality to discover weaknesses in their Process, System or Service to calculate probability of failure and occurrence.

Bottom Up. This view is read upwards, from the fault/cause up to their end effect. All known faults/causes have an undesirable end effect on the Process, System or Service. Using mixed modelling it is possible to combine faults/causes, build in redundancy and/or identify standbys (a mitigating action) enabling reliability and probability of failure to be calculated for known end effects.

This presentation will explore how best to use fault tree analyses to uncover and surface your primary unreliability drivers in your system. We will explore the methodologies and next steps once you have identified the bad actors in your system.

About the presenters, Chris Wynn-Jones and Sam Eisenberg, HBK ReliaSoft Products

Christopher Wynn-Jones has a BEng (Hons) in Mechanical Engineering from University of Wolverhampton coupled with 25 years of engineering experience. After various manufacturing roles Chris went on to become a Safety and Reliability Engineer for civil and military products in the air, at sea and ground vehicles. He is an Application Engineer for ReliaSoft reliability software, supporting customers in industry and in universities with software solutions and best practices in Engineering for Reliability. Chris also sits on the WG1 committee of the Institute of Mechanical Engineers [IMechE] Safety and Reliability Group (SRG). The SRG group promotes the development of safety and reliability requirements for products such as equipment, systems or services.

Sam Eisenberg is the Product Manager for ReliaSoft Products and the Product Owner for ReliaSoft Desktop Products. Sam has been working with ReliaSoft since 2010, beginning with Technical Support, moving into the Application Engineer role, and then taking on the Product Manager / Product Owner roles.

HBK
HOTTINGER BRÜEL & KJÆR

UNRESTRICTED

Fault Tree Analysis

METHODOLOGY AND EFFECTIVE APPLICATION

Prenscia Technology Series 2022

Aims & Objectives

1. Show the scope of linkage between assumptions and external factors through Analysis.
2. Demonstrate the Safety Engineering can influence the Design intent.

Presenters:

- **Chris Wynn-Jones,** *ReliaSoft Application Engineer*
- **Sam Eisenberg,** *Product Manager - ReliaSoft*

www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Agenda

Fault Tree Analysis methodology and effective application

Part 1

a) What is a Fault Tree Analysis [FTA]
b) Top Down view from Safety Analysis – Parallel systems i.e. Safety overrides etc
c) Bottom Up view from Reliability Analysis – example FMEAs serialised

Part 2

a) Common Causes / mirror groups
b) Critical Path / cut sets
c) Identifying missing redundancy [Safety systems/backups]

www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Part 1 – Fault Tree Analysis

Chris Wynn-Jones

 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

Roles

Safety Engineer "Everything Fails"

- Recommending procedures for;
  - Failure detection – Human or autonomous
  - Failure prevention – Fail safe, redundancy
- Elimination of product hazards;
  - Work Schedule / Endurance
  - Physical
  - Chemical
- Minimize or prevent recurrence of;
  - Accidents
  - Injuries
  - Illnesses

Reliability Engineer "It Will Not Fail"

- Identify,
  - Risks / Hazards in a product, system or service
  - Failure Modes
- Perform Reliability Prediction
  - Life Data Analysis
  - Reliability Growth Analysis
- Propose prevention strategy
  - Higher Reliability - 99.999% Reliable @ 1000 yr

  or
  - Maintenance / optimum replacement

In some companies the Safety and Reliability Engineer are the same person

www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

HBK HOTTINGER BRÜEL & KJÆR

CONFIDENTIAL - EXTERNAL

Roles

Safety Engineer "Everything Fails"

- Recommending procedures for;
  - Failure detection – Human or autonomous
  - Failure prevention – Fail safe, redundancy
- Elimination of product
  - Work Schedule / Endurance
  - Physical
  - Chemical
- Minimize or prevent recurrence of;
  - Accidents
  - Injuries
  - Illnesses

Reliability Engineer "It Will Not Fail"

- Identify product, system or service;
  - Risks / Hazards
  - Failure Modes
- Prediction
  - Analysis
  - lity Growth Analysis
- Prevention
  - High Reliability - 99.999% Reliable @ 1000 yr

or

  - Maintenance strategy

The fault tree offers a common tool where both roles contribute to the same work flow

In some companies the Safety and Reliability Engineer are the same person

 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

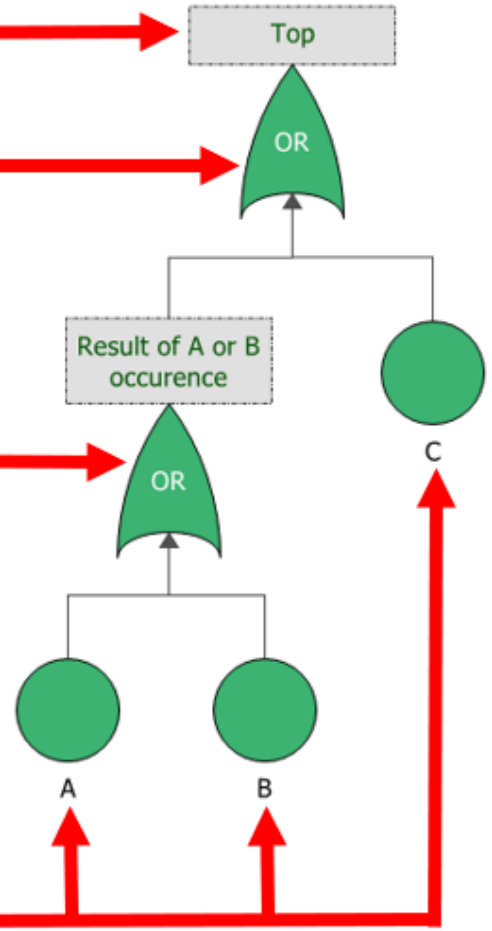
What is a fault tree?

- A fault tree diagram is a graphical model of the pathways within a Product, System or Service that can lead to an undesirable event.

The highest-level event (output event) being analyzed.

Logic symbols that interconnect contributory events and conditions in a fault tree diagram. They dictate how the chains of events propagate through the fault tree.

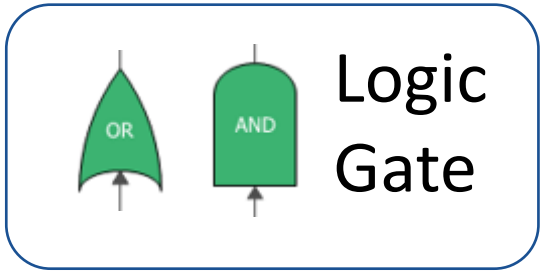
Contributors/initiators (e.g. failures, human error) at the lowest level of granularity set for the analysis. They are the inputs to the gate.



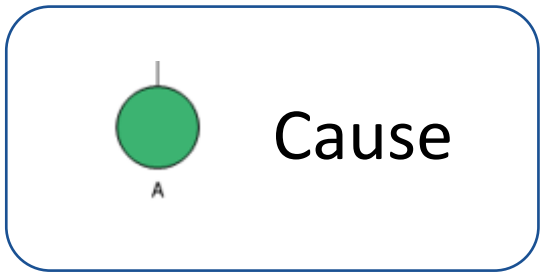
CONFIDENTIAL - EXTERNAL

Fault tree basic elements

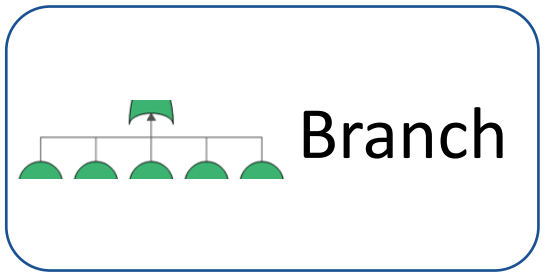
- Logic Gate
  - These are used to represent the behaviour of the different elements in a Product , System or Service. With these we can picture how everything works together.



- Contributor / Cause
  - Failure Mode, Event or Item at the lowest level of granularity.



- Branch
  - Cluster or sub tree structure linking contributors to a failure stage together.

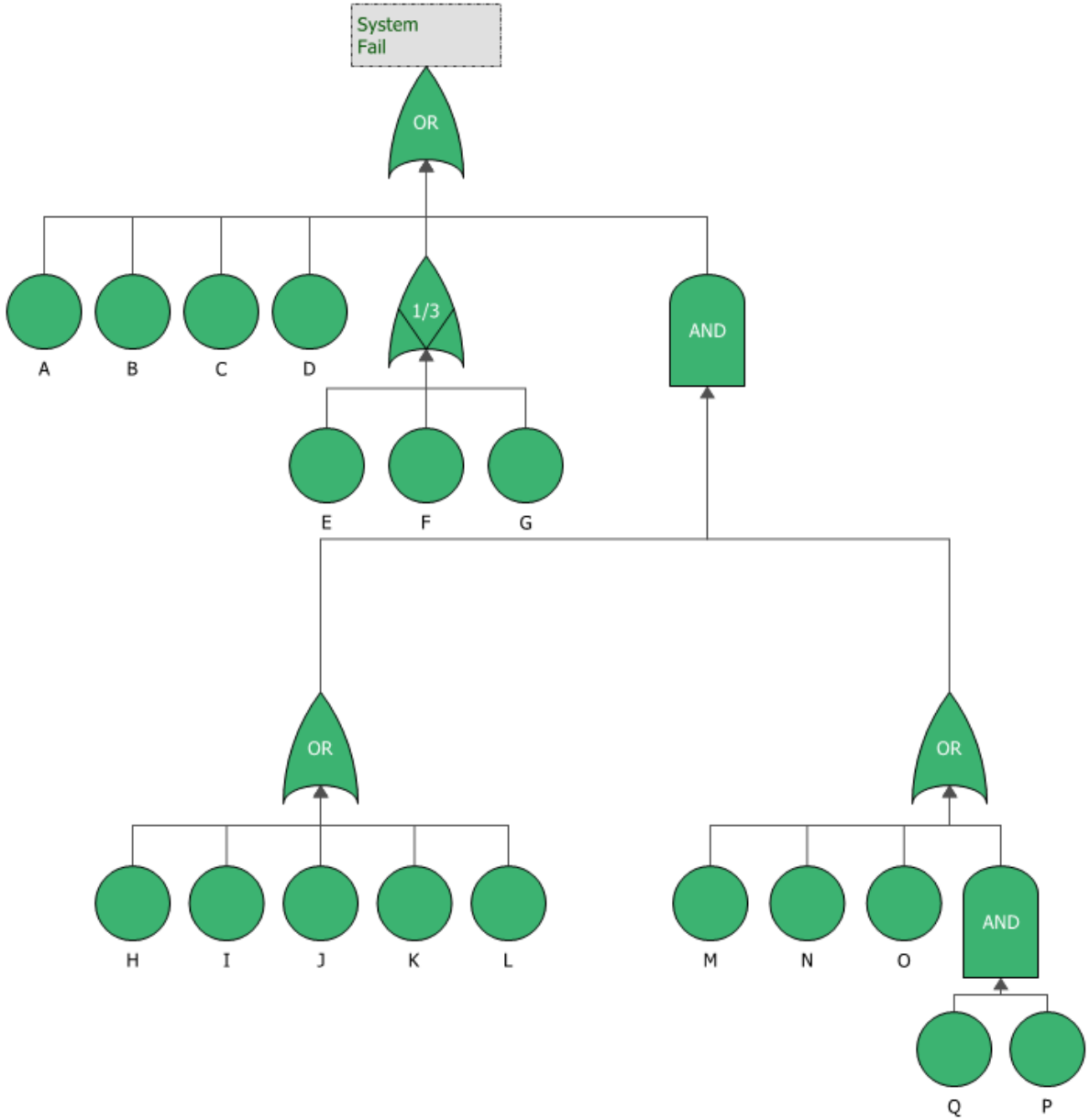


www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.



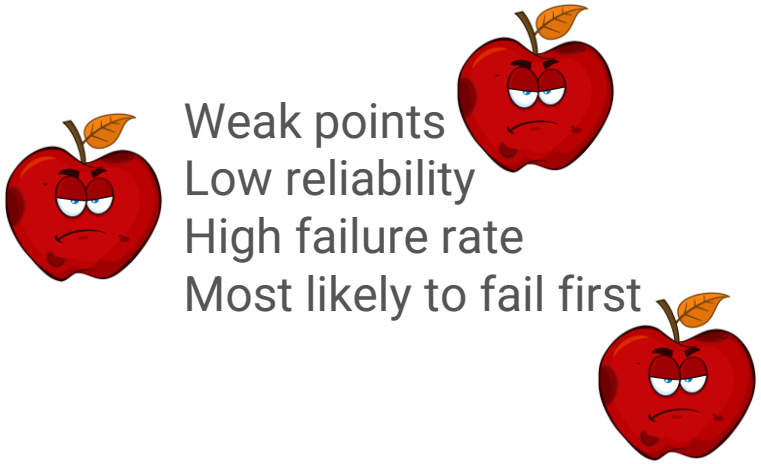
 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

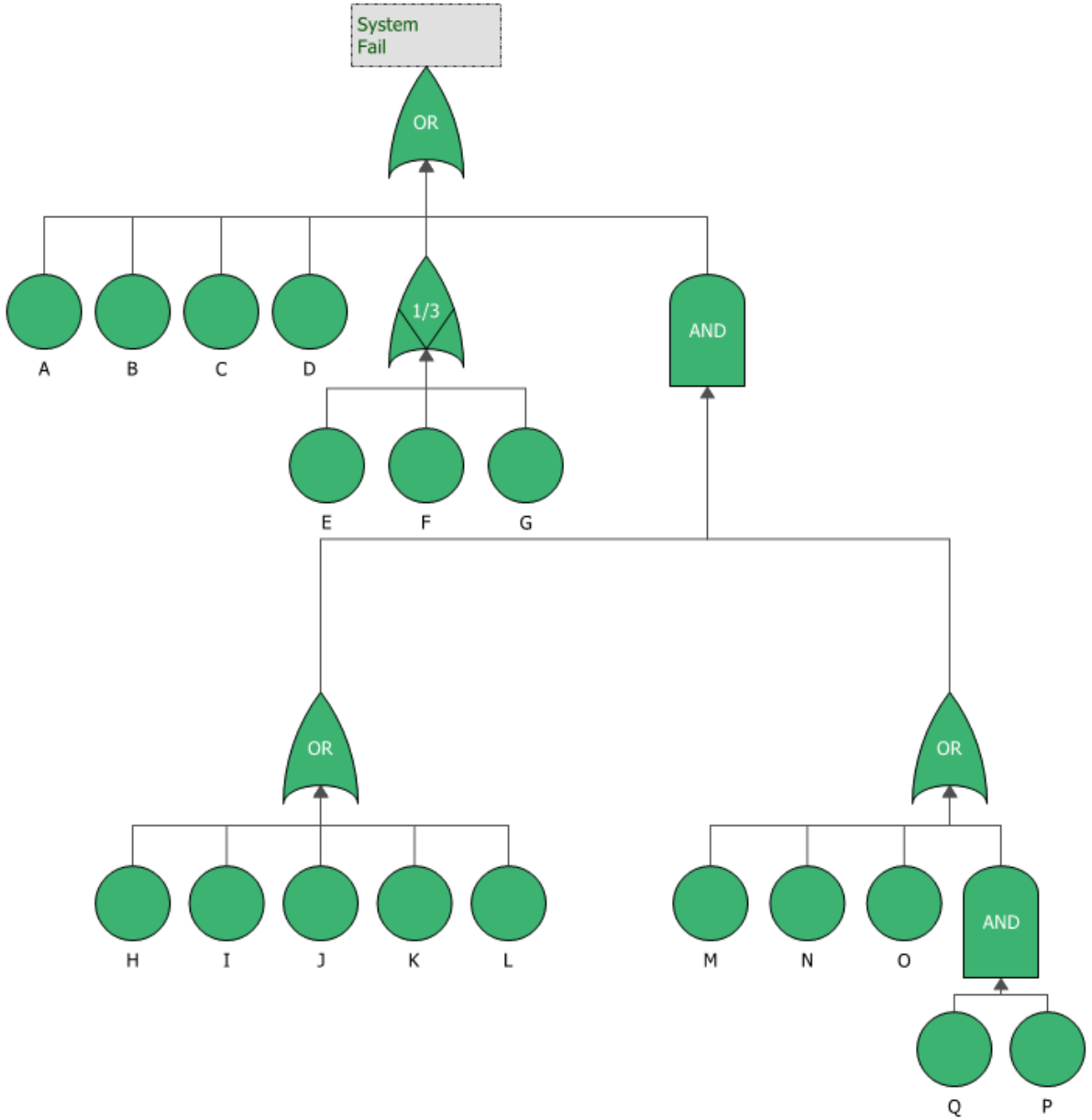
What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.

Let me introduce the Bad Apples;



Weak points
Low reliability
High failure rate
Most likely to fail first



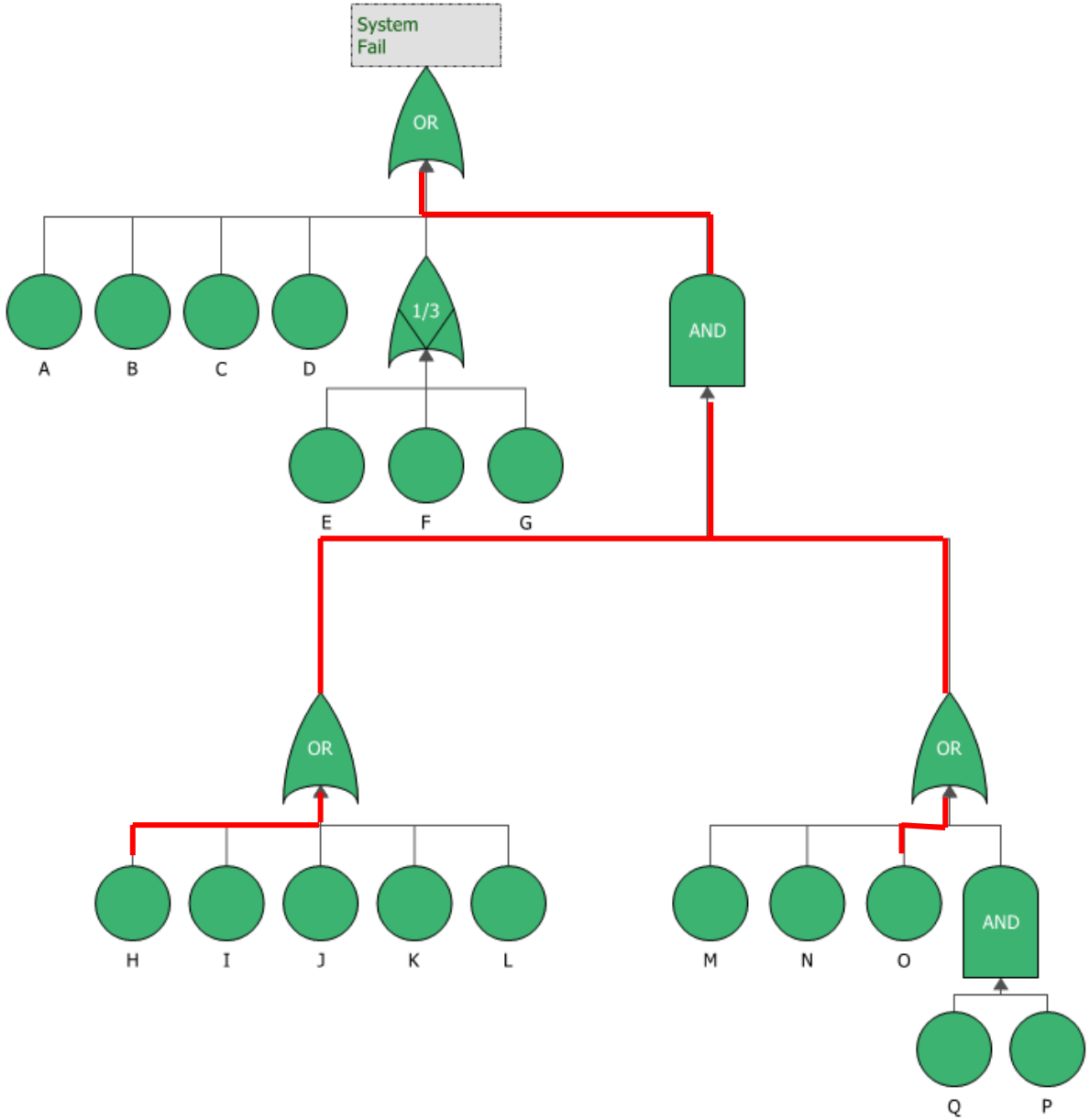
 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.

A fault tree diagram is a graphical representation used to identify the pathways within a Product, System or Service that can lead to an undesirable event or failure.



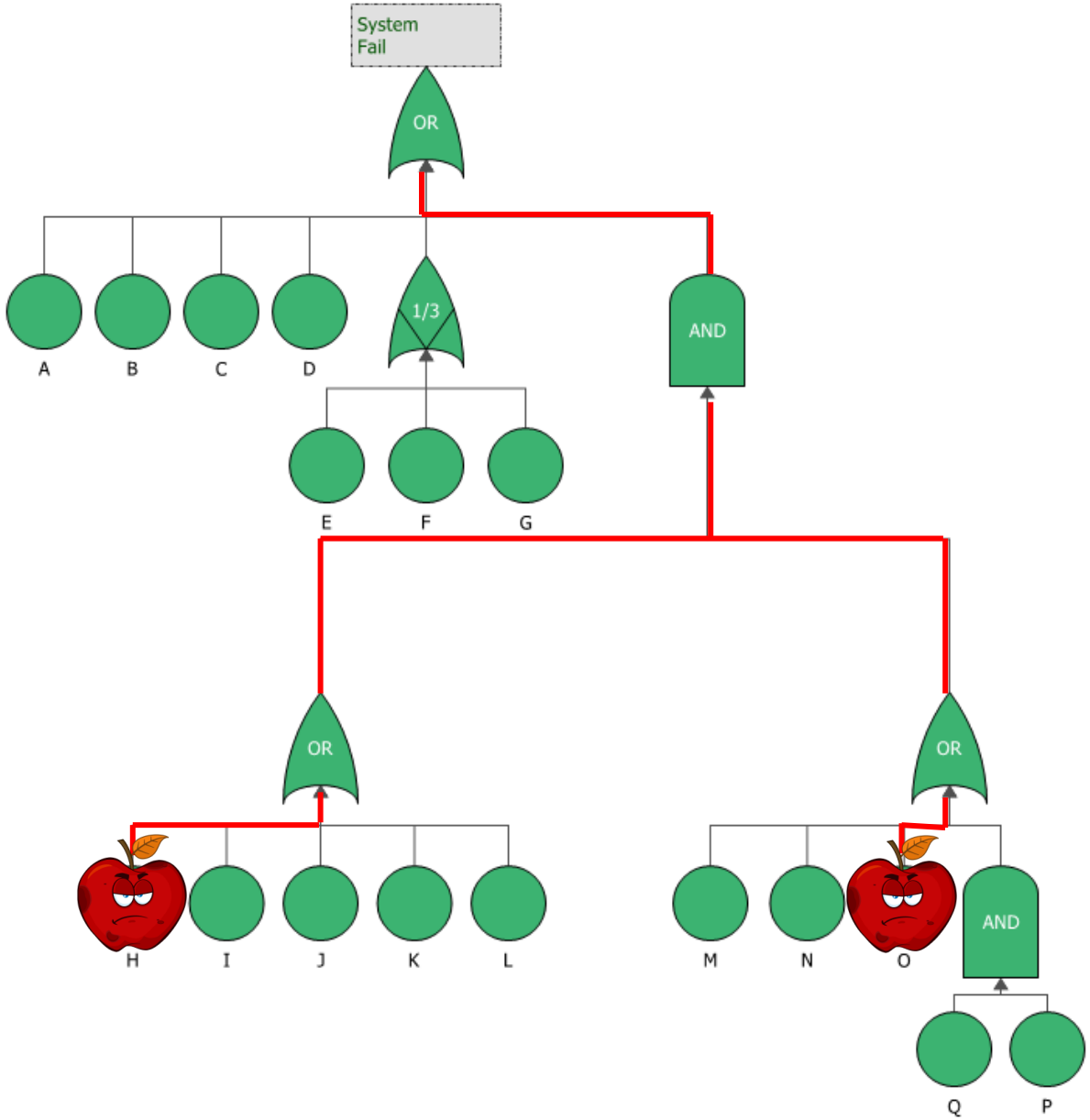
 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.

A fault tree diagram is a graphical representation used to identify the pathways within a Product, System or Service that can lead to an undesirable event or failure.



 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

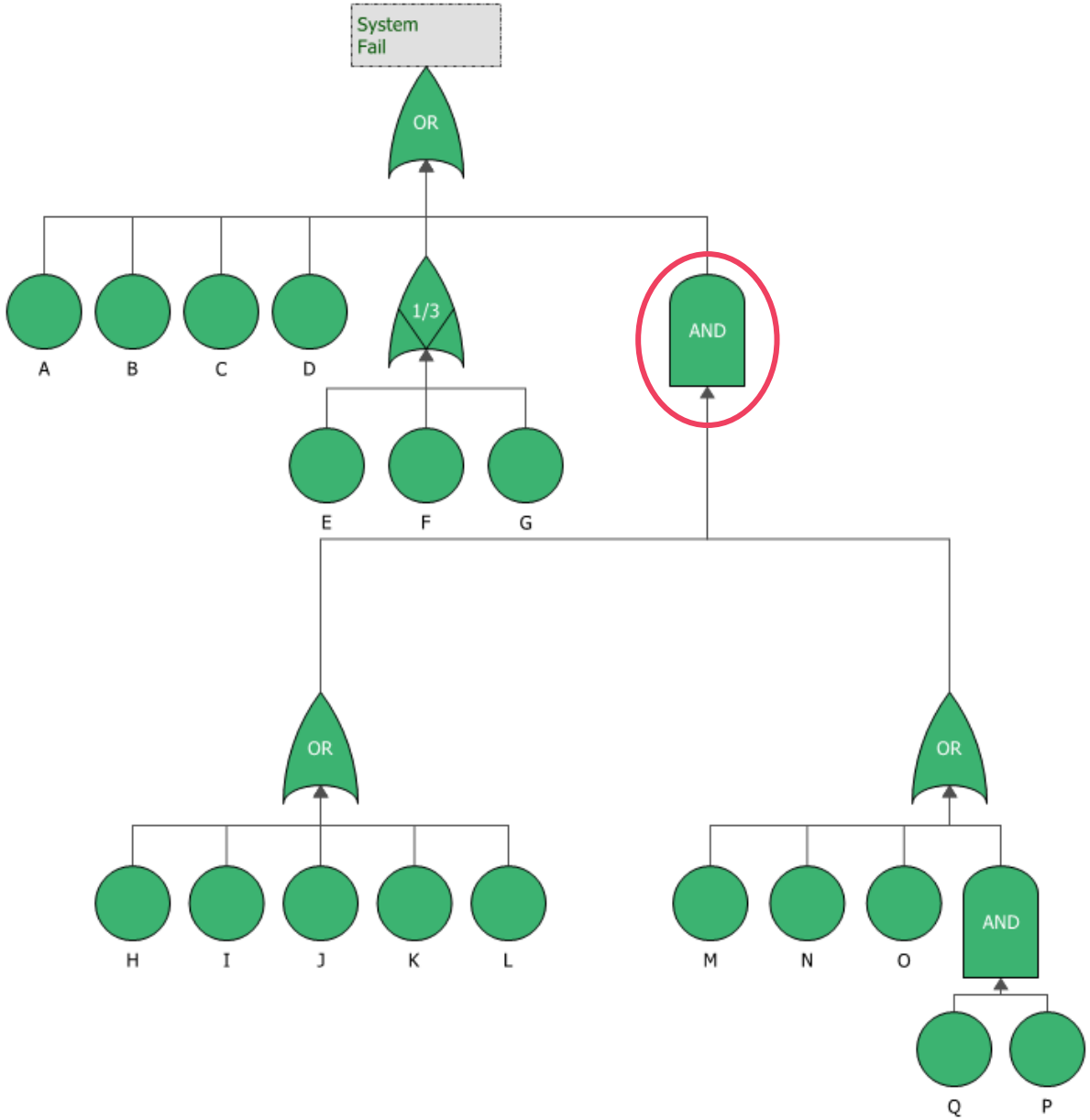
CONFIDENTIAL - EXTERNAL

What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.

A fault tree diagram is a graphical representation used to identify the pathways within a Product, System or Service that can lead to an undesirable event or failure.

These pathways connect up contributors and conditions (A to P) using standard logic gates (AND, OR, etc).



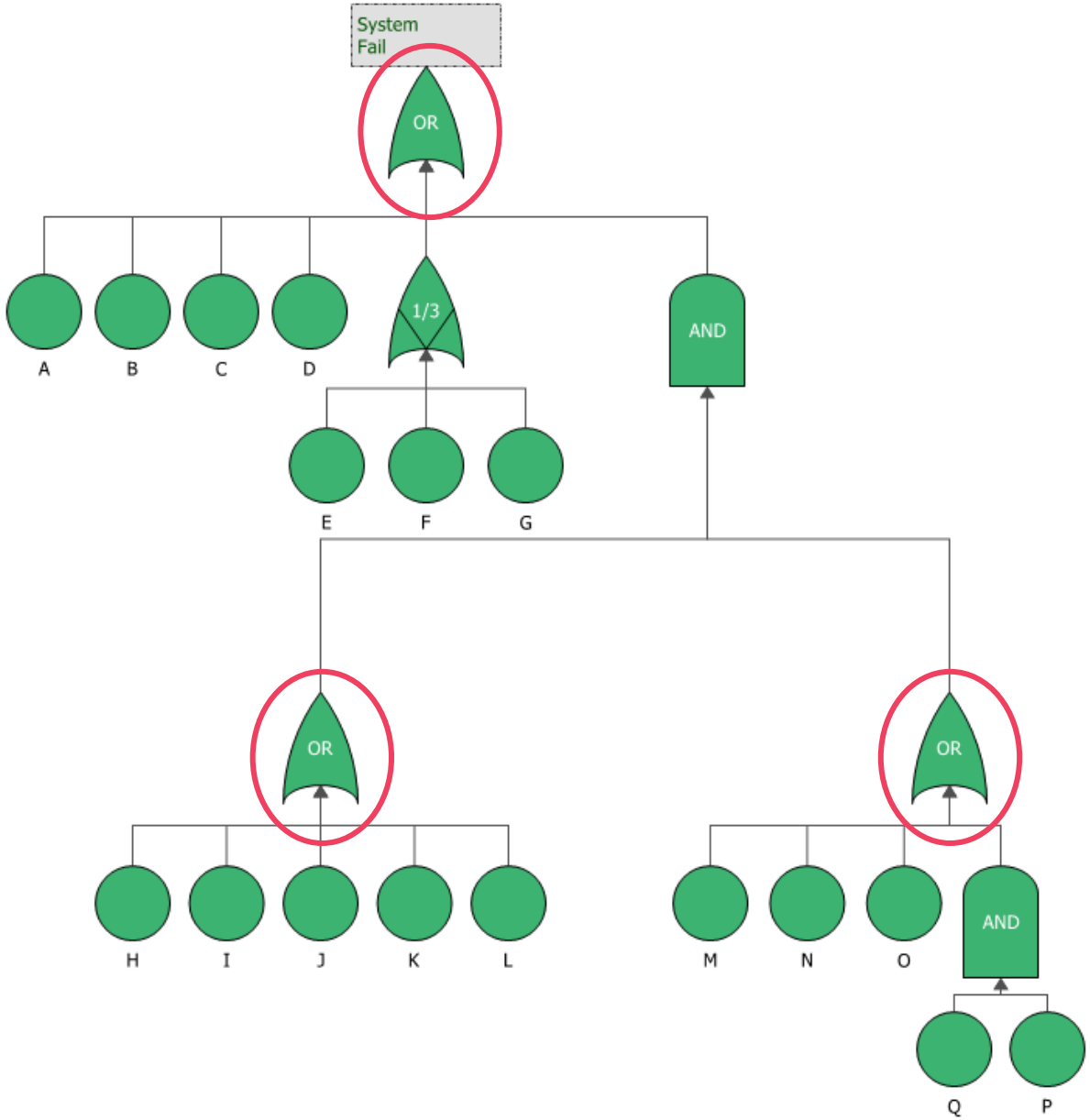
CONFIDENTIAL - EXTERNAL

What is fault tree analysis (FTA)?

Fault tree analysis is one of many symbolic "analytical logic techniques" found in many disciplines.

A fault tree diagram is a graphical representation used to identify the pathways within a Product, System or Service that can lead to an undesirable event or failure.

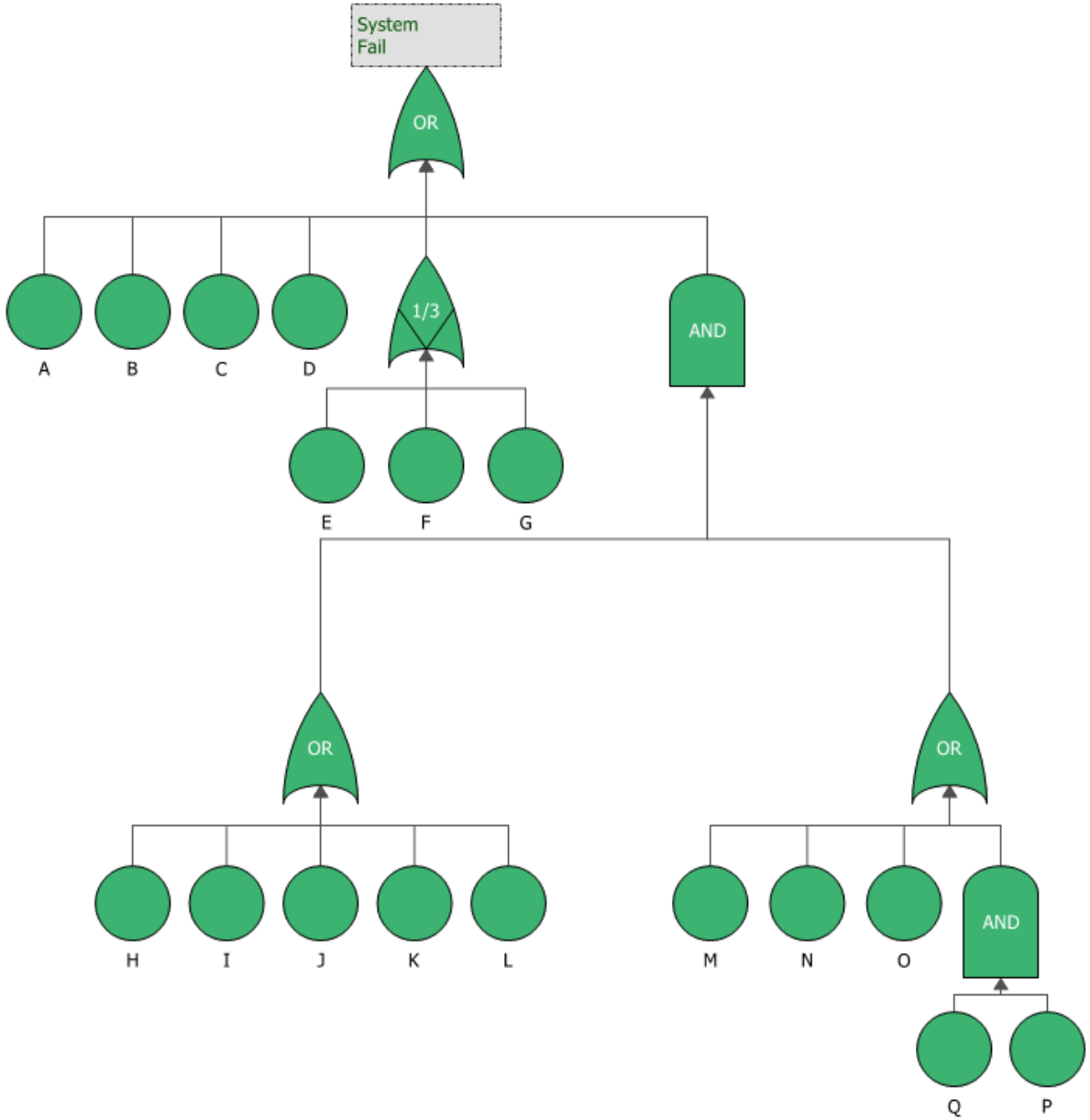
These pathways connect up contributors and conditions (A to P) using standard logic gates (AND, OR, etc).



CONFIDENTIAL - EXTERNAL

Top-Down approach

Fault trees can be required following a Safety concern, or maybe a failure of a Product, System or Service during operation.



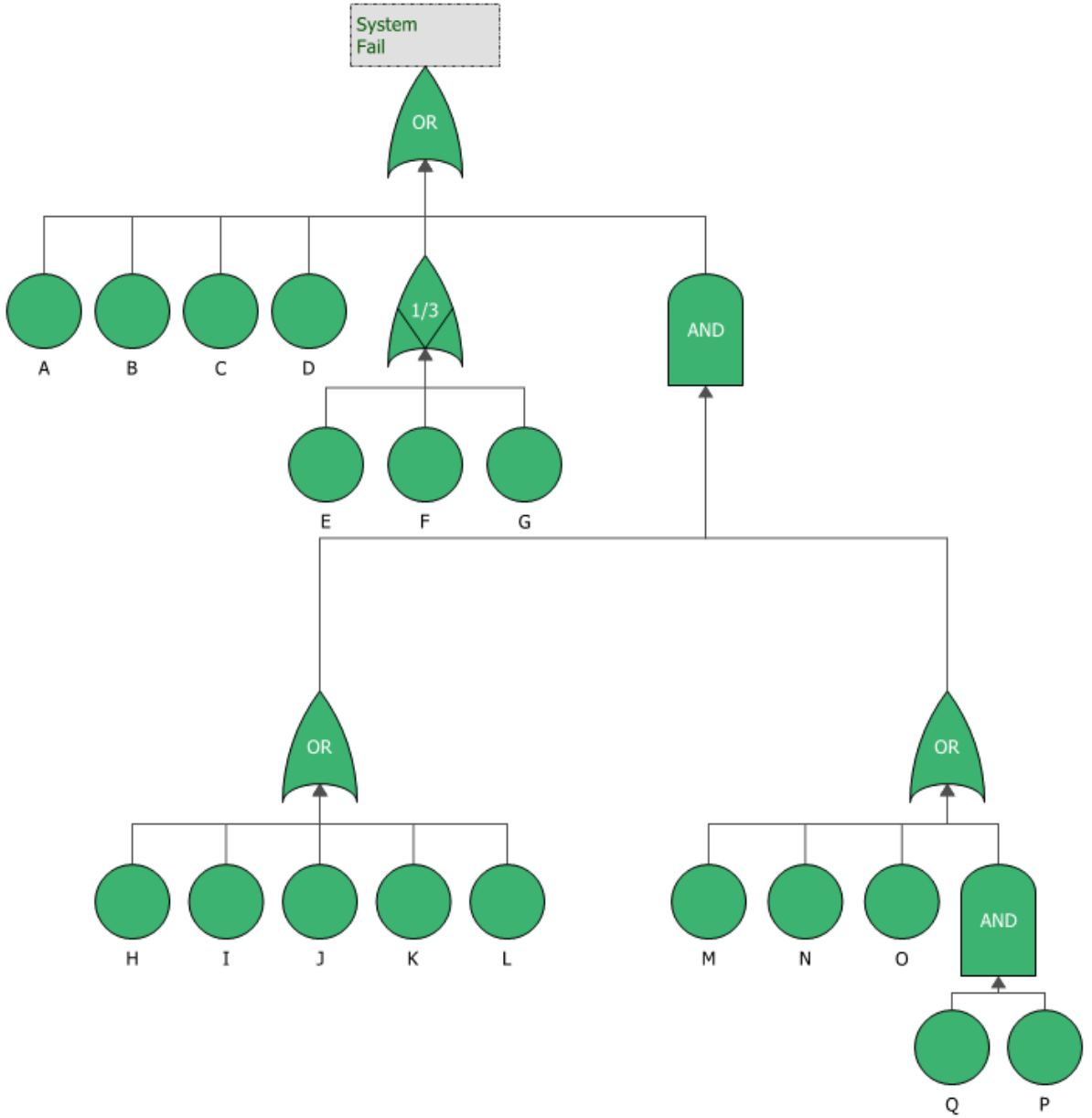
 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Top-Down approach

Fault trees can be required following a Safety concern, or maybe a failure of a Product, System or Service during operation.

The undesirable event is set at the top the fault tree and the analysis is build down as each contributor is discovered. This approach is known as the Top-Down approach and allows the analyst to find the most likely contributors that result in failure.



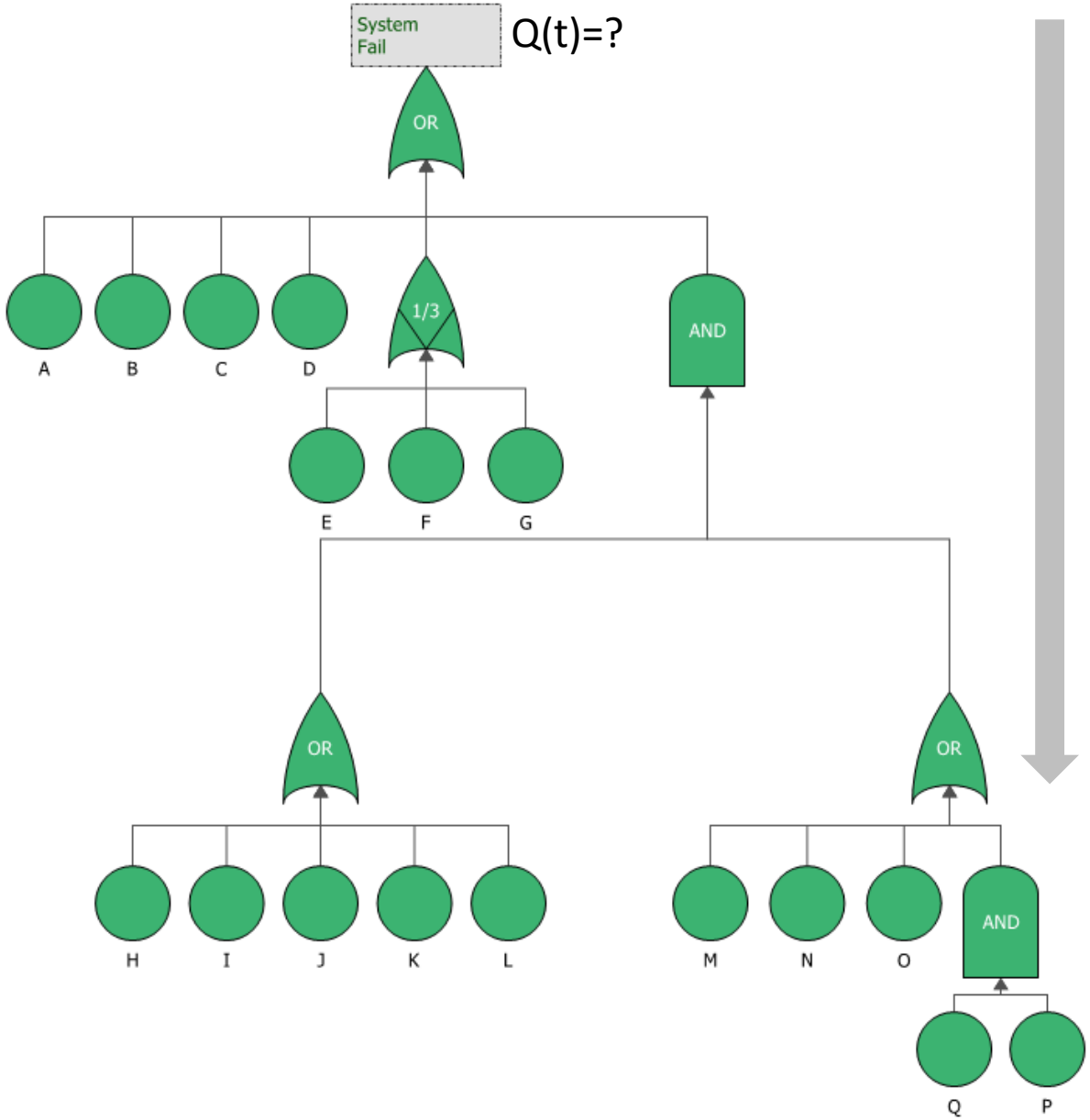
CONFIDENTIAL - EXTERNAL

Top-Down approach

Fault trees can be required following a Safety concern, or maybe a failure of a Product, System or Service during operation.

The undesirable event is set at the top the fault tree and the analysis is build down as each contributor is discovered. This approach is known as the Top-Down approach and allows the analyst to find the most likely contributors that result in failure.

The failure rate (Q) can be found at each level and the lowest values become the main focal point for that part of the tree [Critical Path].

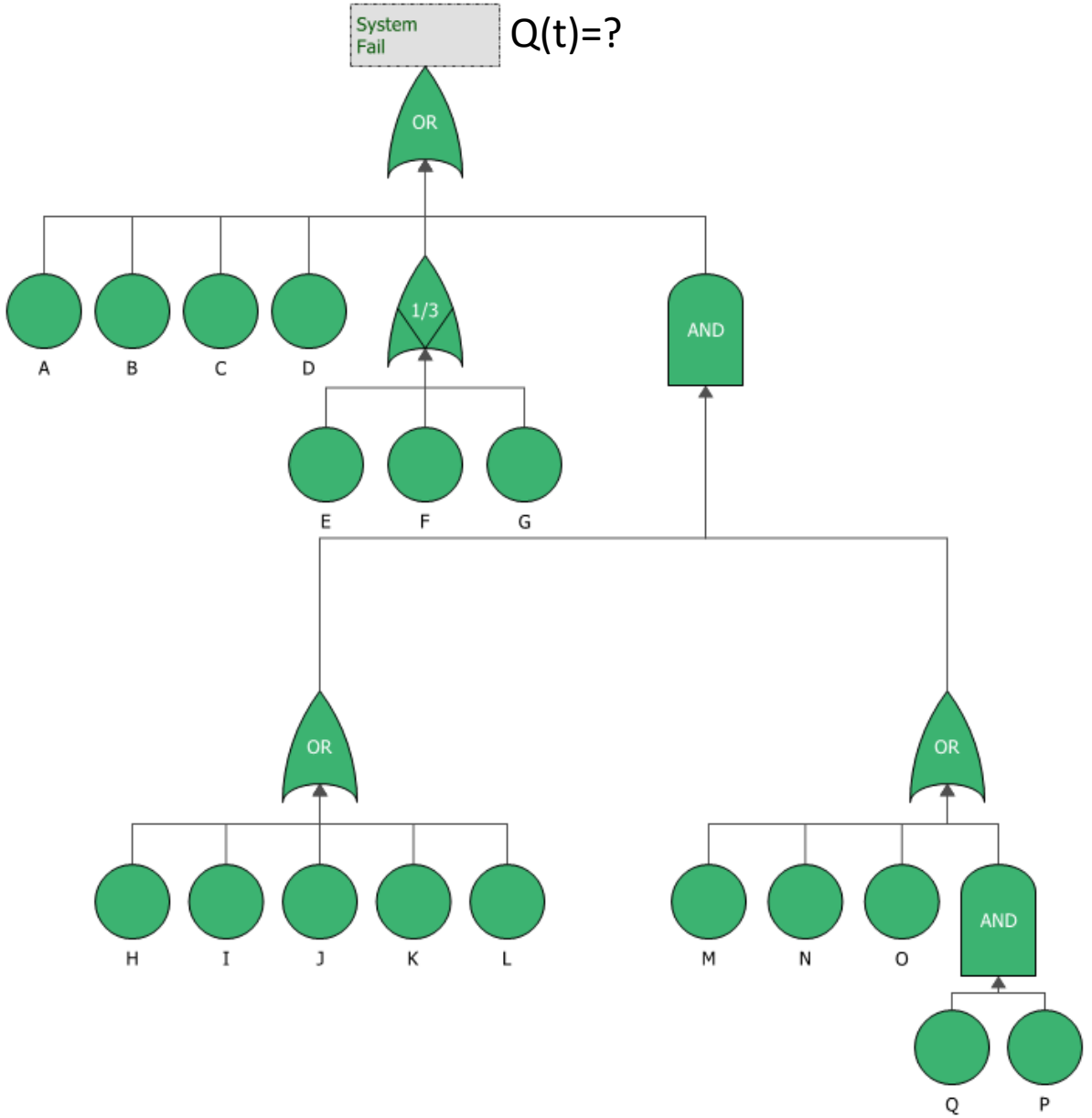


www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Calculating Q - Unreliability

Q(t) = Unreliability or probability of failure = **1-R(t)**



 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

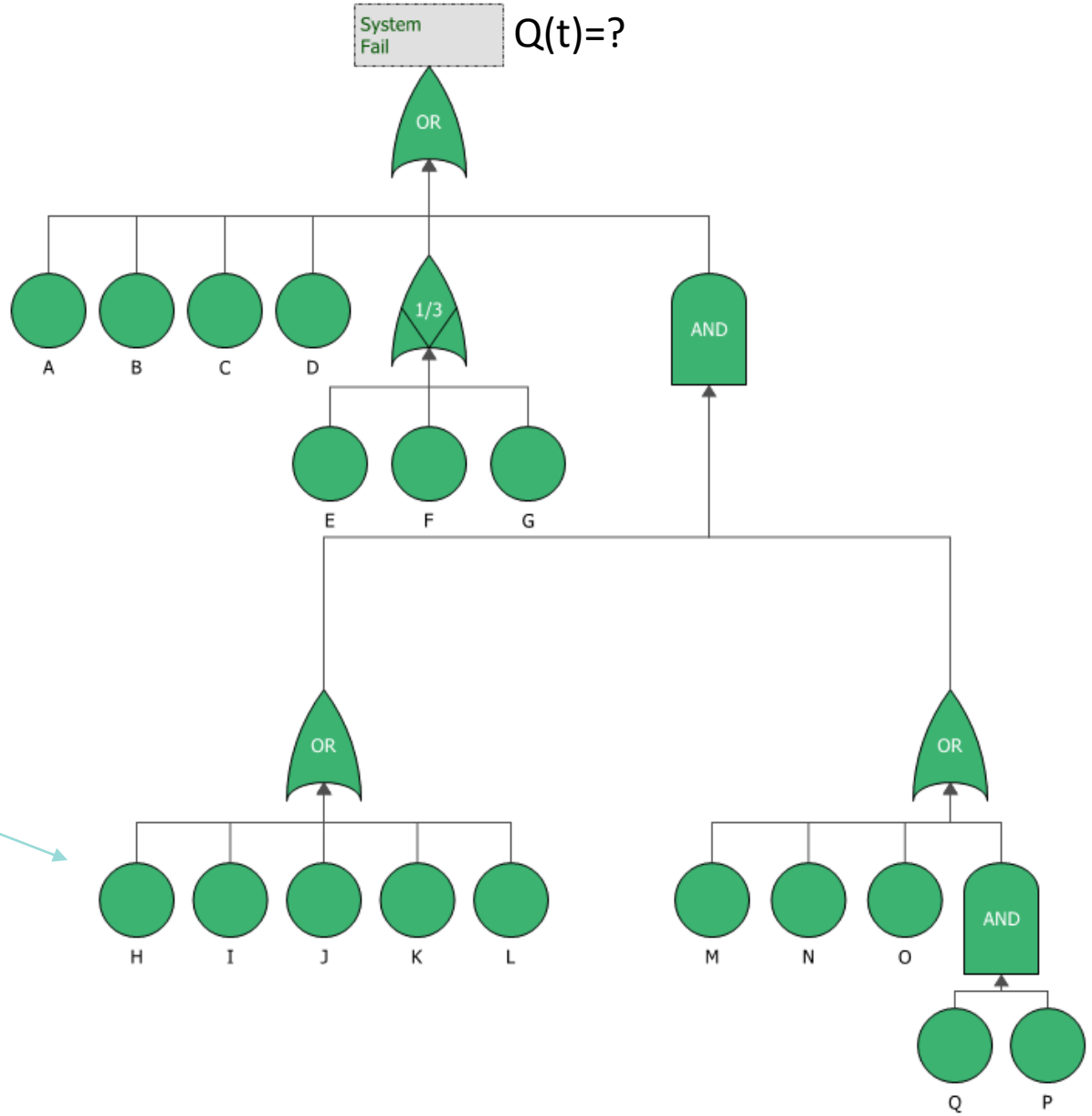
Calculating Q - Unreliability

Q(t) = Unreliability or probability of failure = **1-R(t)**

Example;

Causes H to L each have a calculated value for R at a given time (t) … $R = e^{-\lambda t}$, the **OR** multiples then giving Q(t) for this branch of the FTA.

H[1-R(t)] x I[1-R(t)] x ……



www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Calculating Q - Unreliability

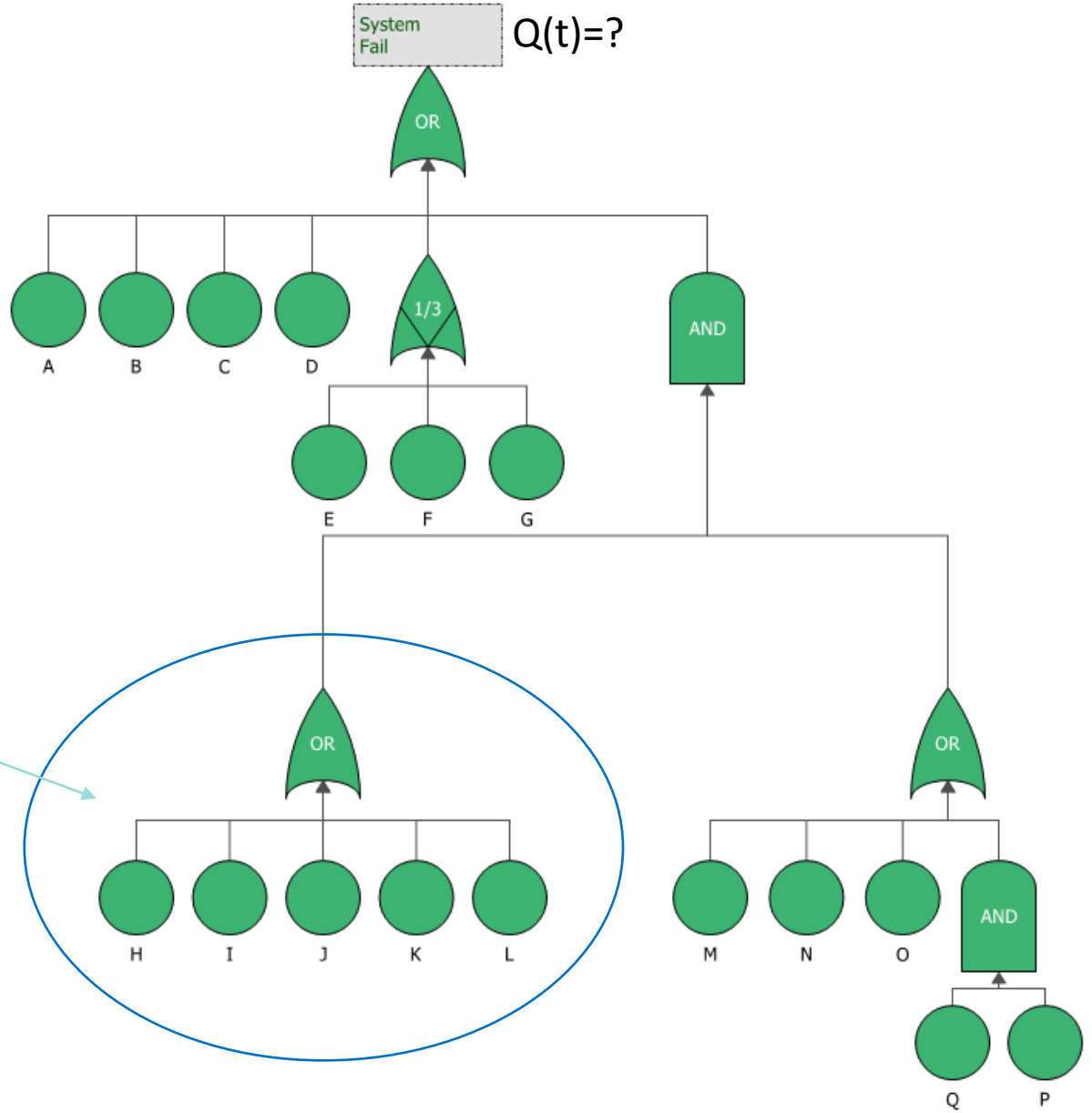
Q(t) = Unreliability or probability of failure = **1-R(t)**

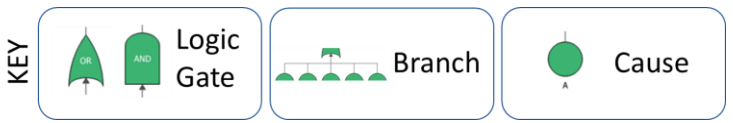
Example;

Causes H to L each have a calculated value for R at a given time (t), … $R = e^{-\lambda t}$, the **OR** multiples then giving Q(t) for this branch of the FTA.

H[1-R(t)] x I[1-R(t)] x J[1-R(t)] x I[1-R(t)] x J[1-R(t)]

= Z[Q(t)]





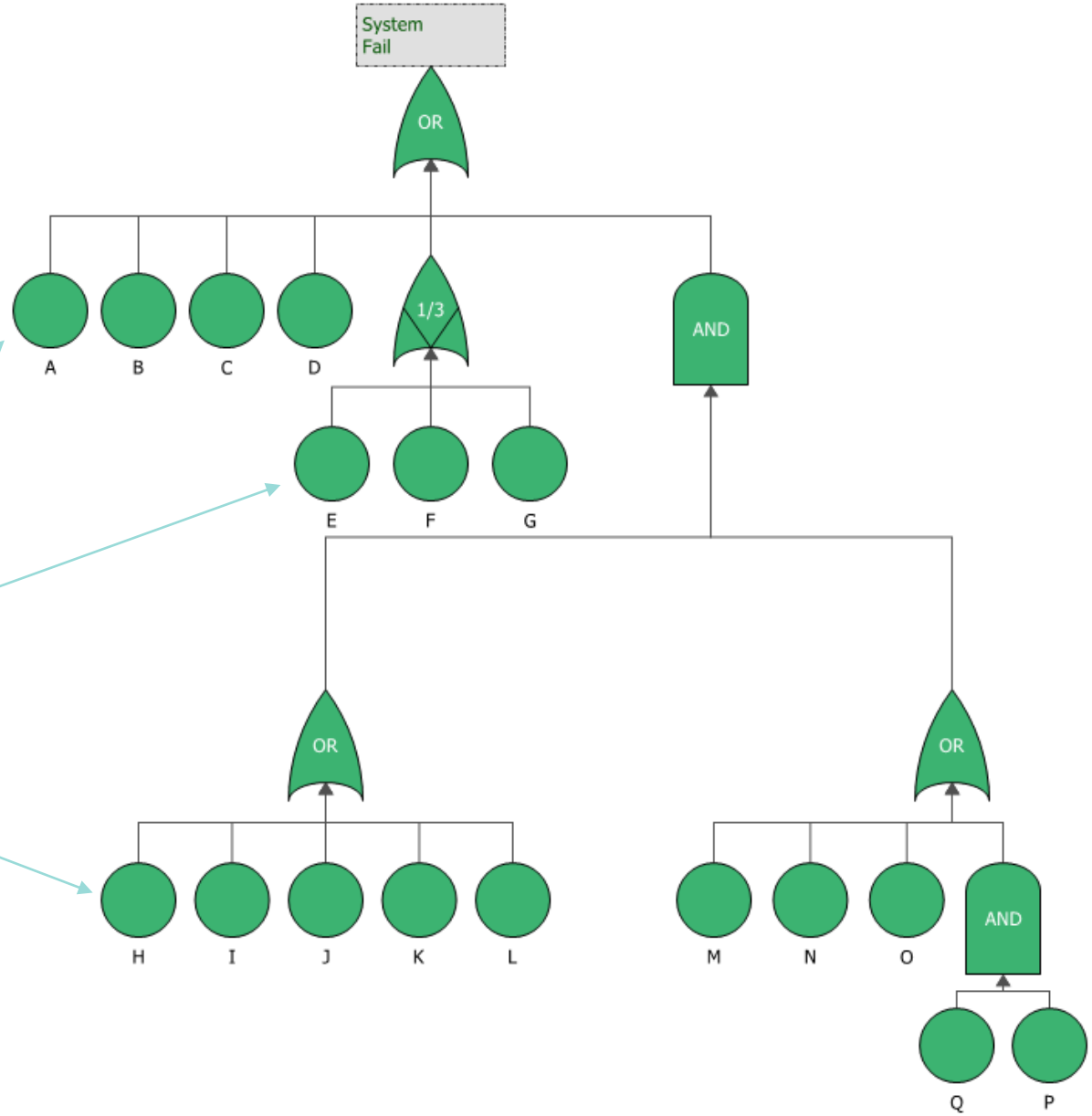
CONFIDENTIAL - EXTERNAL

Bottom-Up approach

Fault trees may also be useful for analyzing the effects of individual failure modes and in conjunction with Failure Mode and Effects Analysis [FMEA].

FMEA

Function / Failure / Effect / **Causes** / Controls & **Statistics**



KEY

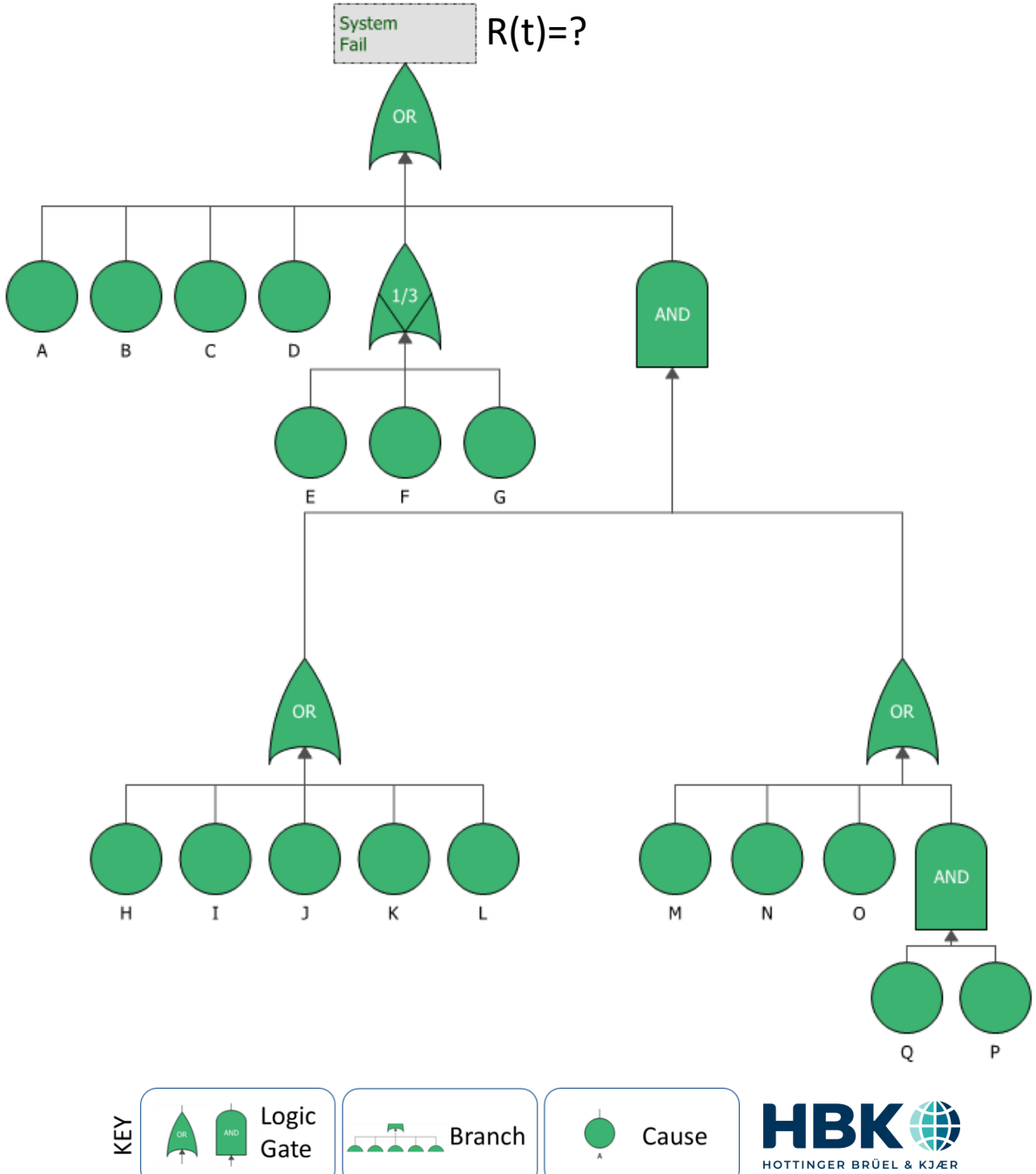
Logic Gate | Branch | Cause

CONFIDENTIAL - EXTERNAL

Bottom-Up approach

Fault trees may also be useful for analyzing the effects of individual failure modes and in conjunction with Failure Mode and Effects Analysis [FMEA].

Identified failure modes from the FMEA lead to component failures and then result in the Product, System or Service failing. Failure data is used to calculate a Reliability (R) for the failure modes.



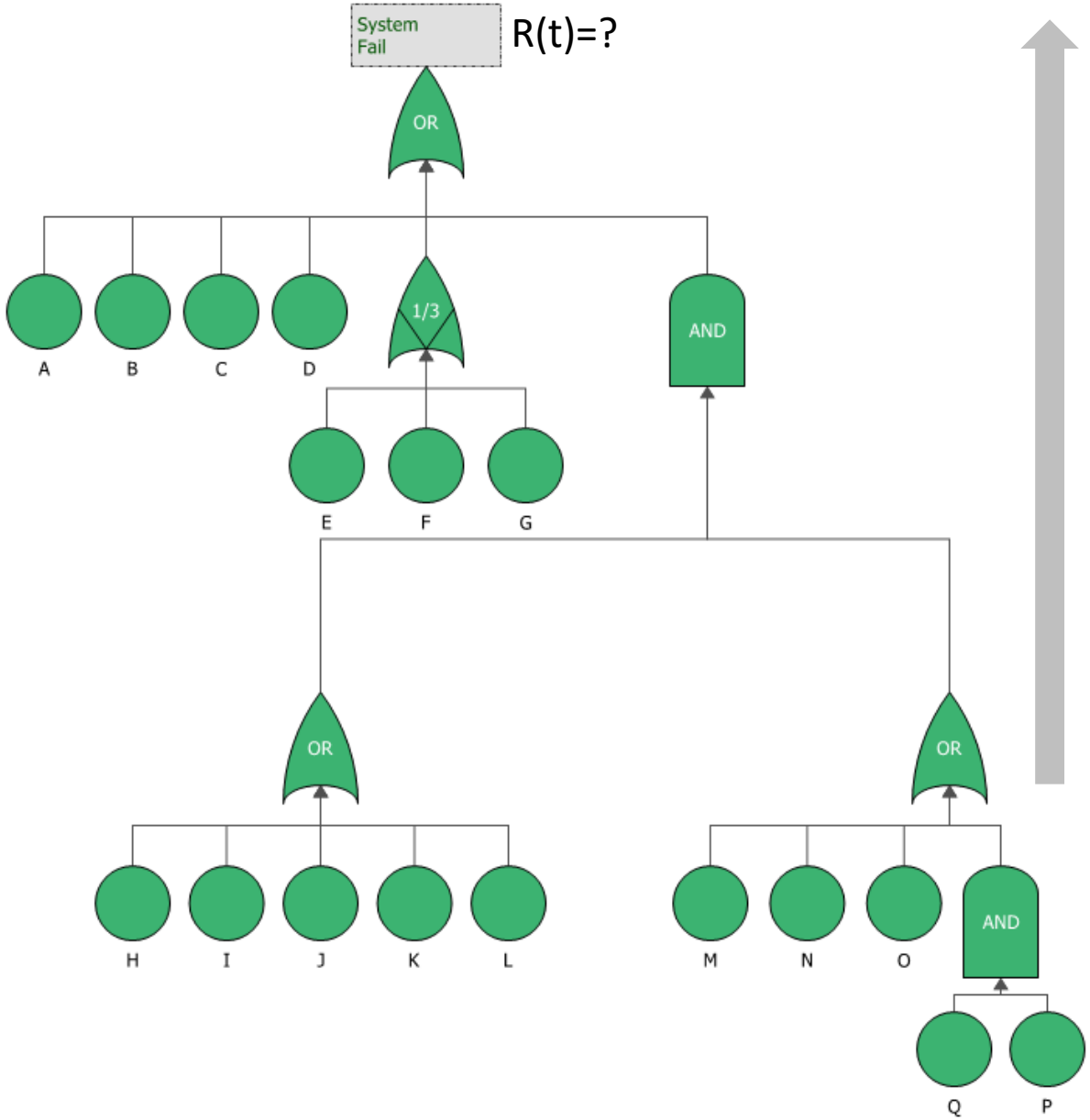
CONFIDENTIAL - EXTERNAL

Bottom-Up approach

Fault trees may also be useful for analyzing the effects of individual failure modes and in conjunction with Failure Mode and Effects Analysis [FMEA].

Identified failure modes from the FMEA lead to component failures and then result in the Product, System or Service failing. Failure data is used to calculate a Reliability (R) for the failure modes.

The Analyst starts the failure mode data and hierarchy to build the fault tree up to the highest actionable point of failure. This is known as the Bottom-up approach.



CONFIDENTIAL - EXTERNAL

Calculating R - Reliability

The flip to unreliability, **R(t)** = Reliability

I want to know my reliability with all know causes in play

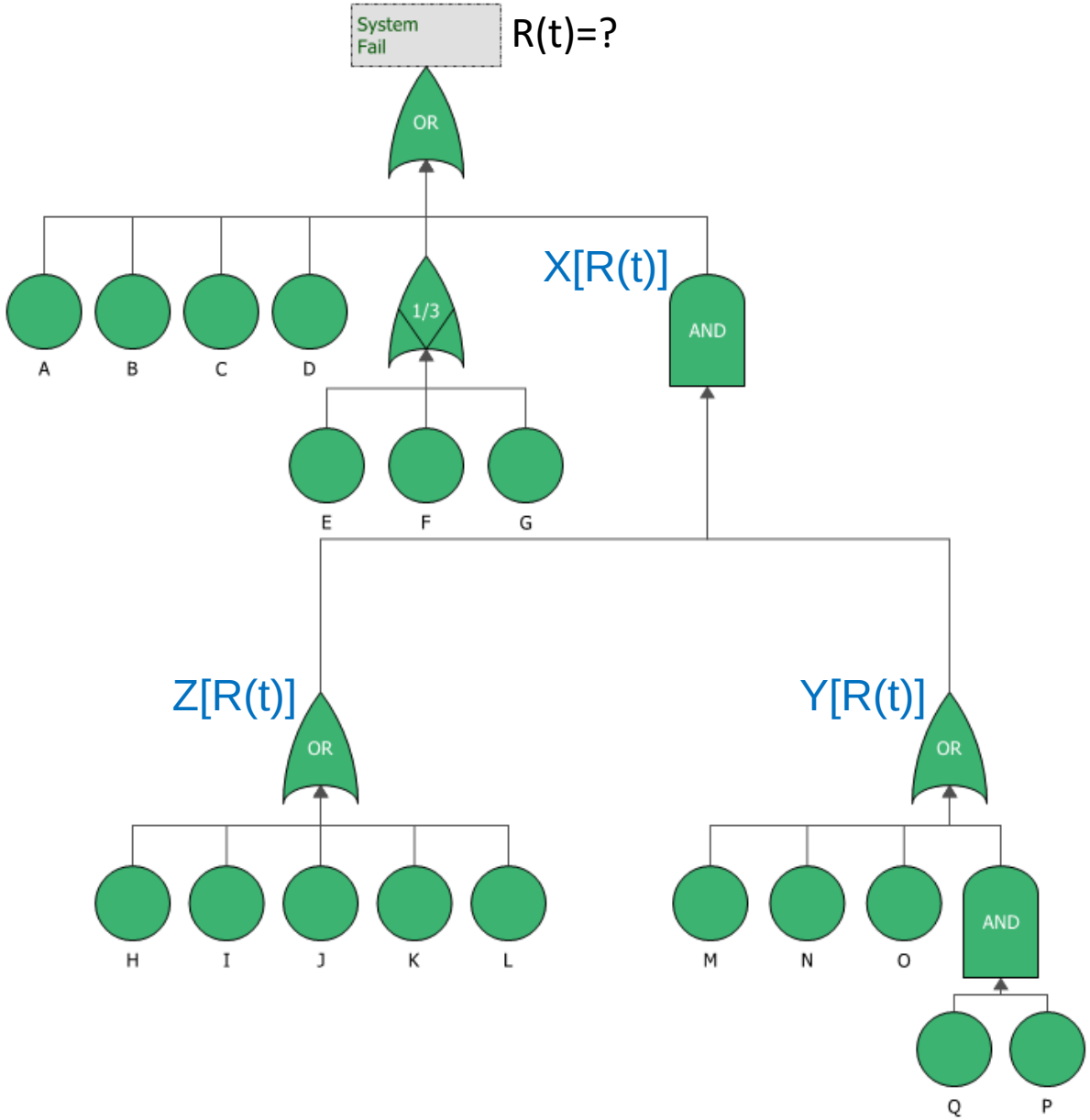
Example;

Causes H to L each have a calculated value for R at a given time (t), the **OR** multiples then giving R(t) for this branch of the FTA.

H[R(t)] x I[R(t)] x J[R(t)] …… = Z[R(t)]

At he **AND** gate the outputs are added,

Z[R(t)] + Y[R(t)] = X[R(t)]

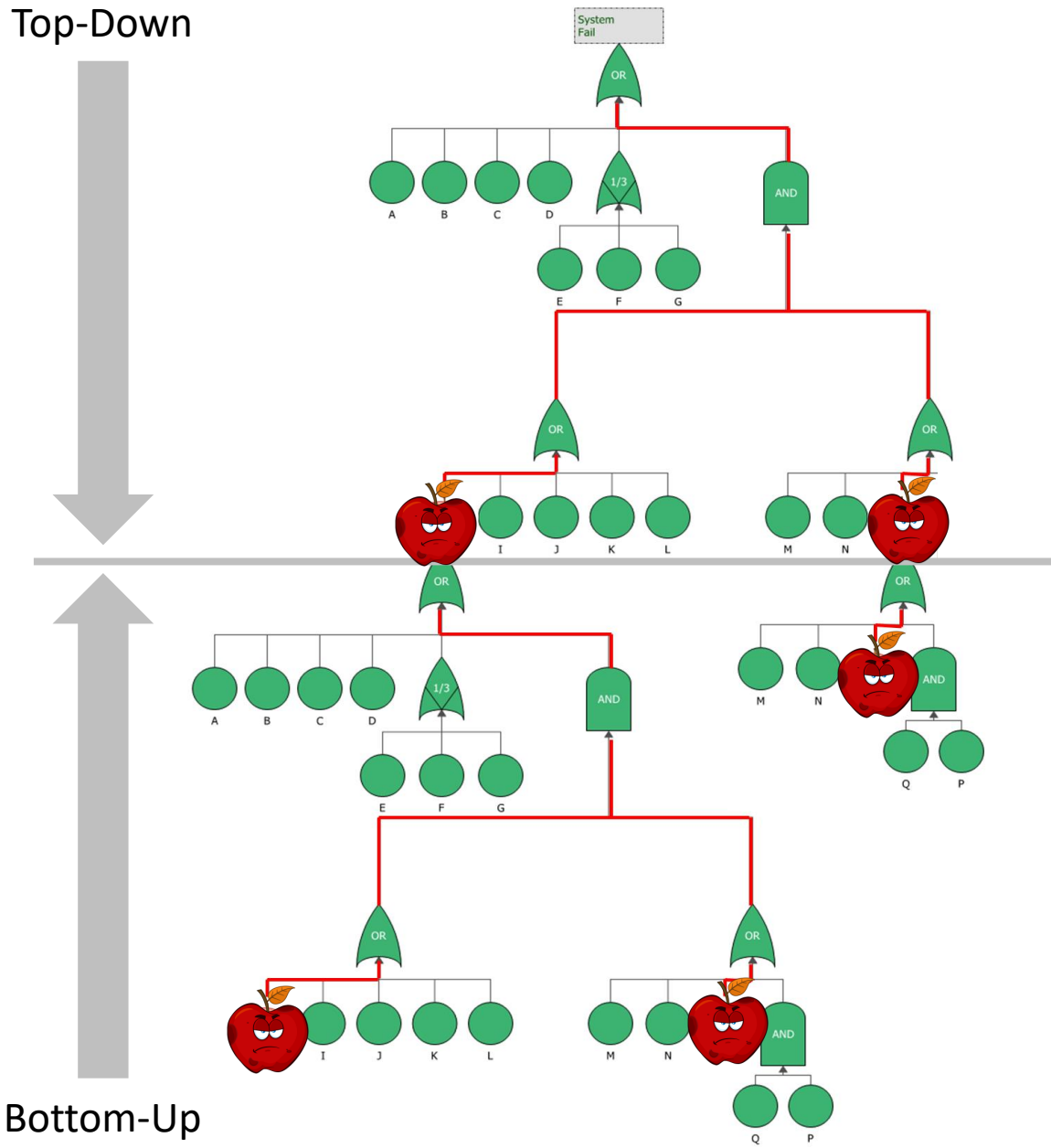


 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Where both approaches meet

The Safety Analyst and Reliability Analyst both use the same tool but for different directions.



 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

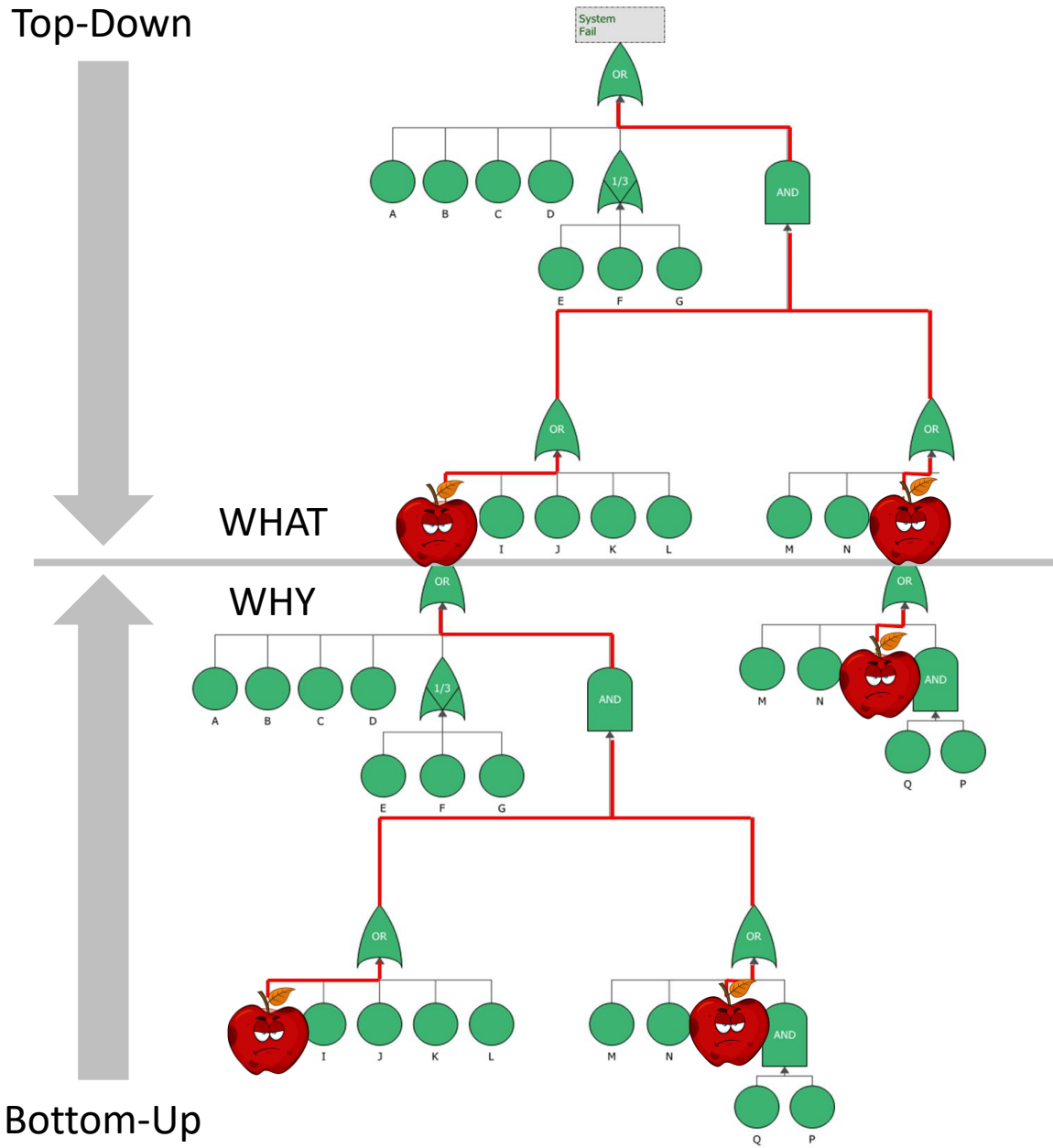
CONFIDENTIAL - EXTERNAL

Where both approaches meet

The Safety Analyst and Reliability Analyst both use the same tool but for different directions.

Top-Down, the Safety Engineers view takes an incident or failure and finds out what the most likely culprit could be.

Bottom-Up, the Reliability Engineer's analysis of the known causes within a Product, System or Service that could contribute to its failure.



 www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

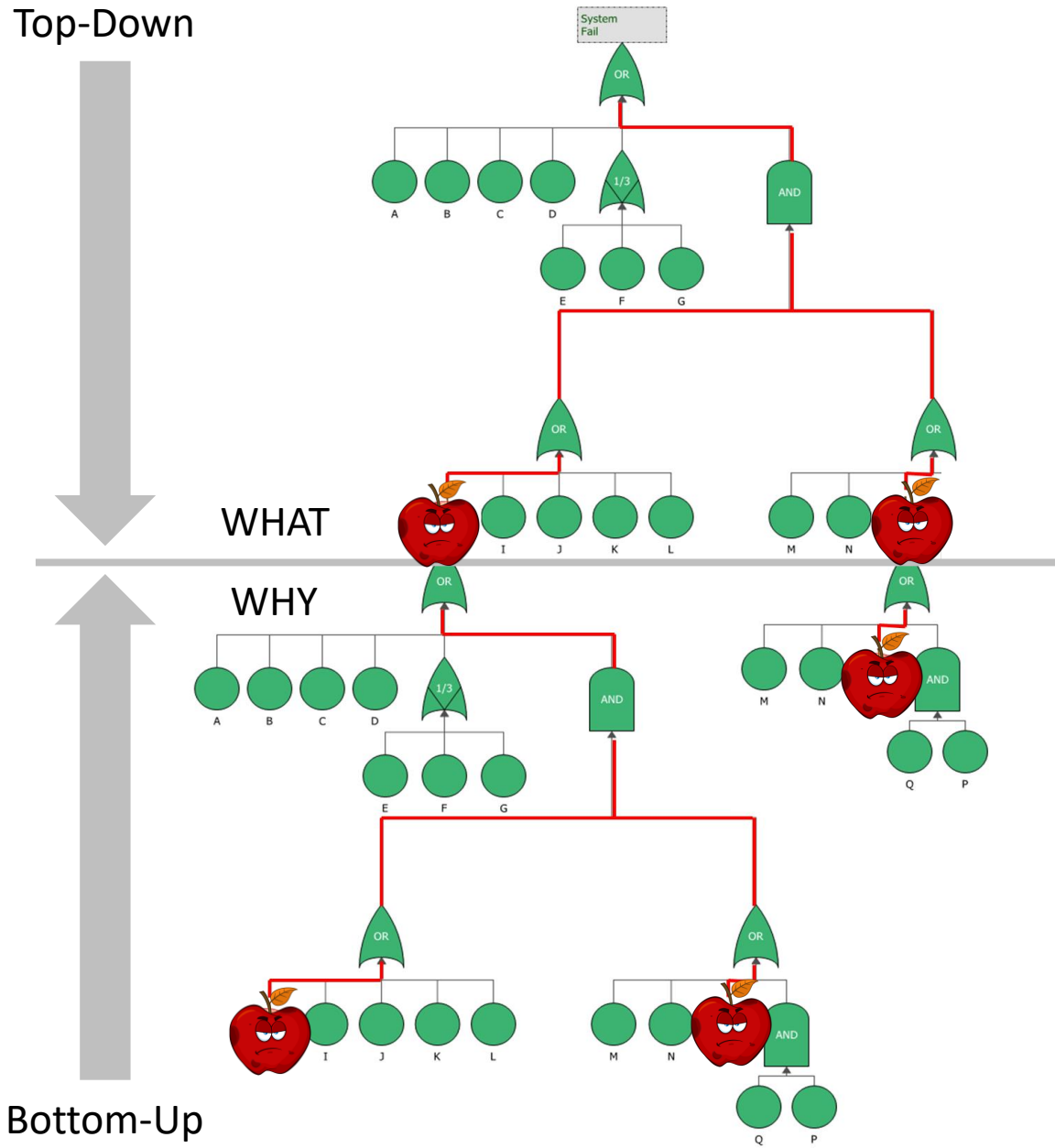
Where both approaches meet

The Safety Analyst and Reliability Analyst both use the same tool but for different directions.

Top-Down, the Safety Engineers view takes an incident or failure and finds out what the most likely culprit could be.

Bottom-Up, the Reliability Engineer's analysis of the known causes within a Product, System or Service that could contribute to its failure.

There is in most cases an overlap between these approaches, the point where they meet moves up and down depending on the level of knowledge that exists at the time the analysis was carried out.



CONFIDENTIAL - EXTERNAL

Where both approaches meet

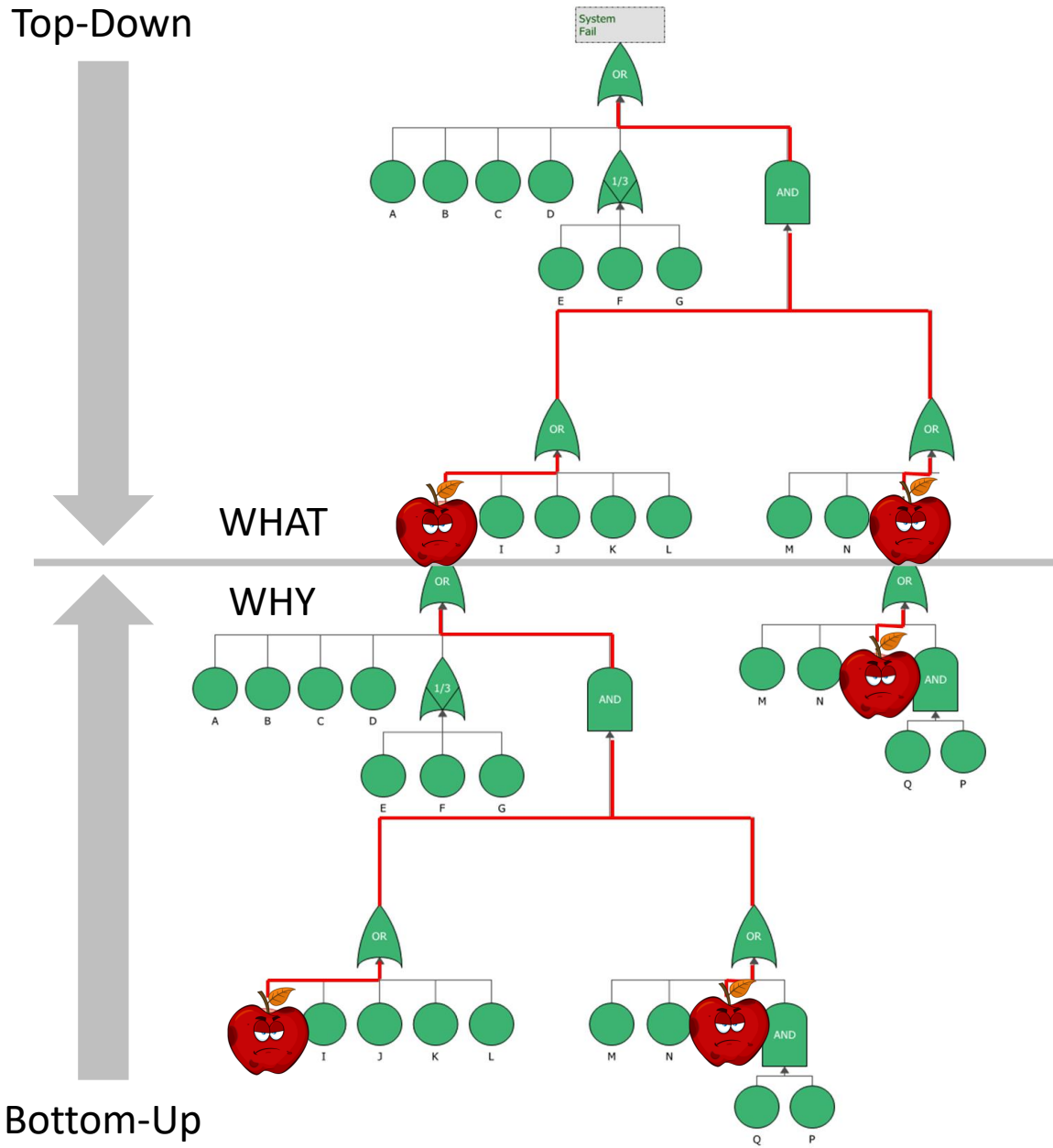
The Safety Analyst and Reliability Analyst both use the same tool but for different directions.

Top-Down, the Safety Engineers view takes an incident or failure and finds out what the most likely culprit could be.

Bottom-Up, the Reliability Engineer's analysis of the known causes within a Product, System or Service that could contribute to its failure.

There is in most cases an overlap between these approaches, the point where they meet moves up and down depending on the level of knowledge that exists at the time the analysis was carried out.

Depending on the customer and supplier relationship this overlap can be subject to contract and data protection for information availability.



CONFIDENTIAL - EXTERNAL

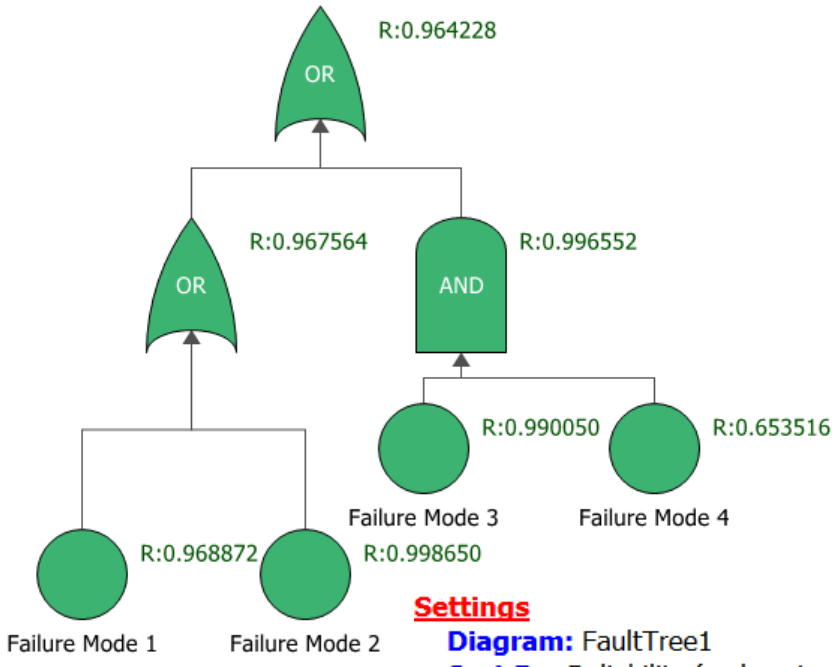
Part 2 – Fault Tree Analysis continued

Sam Eisenberg

 | © HBK – Hottinger, Brüel & Kjær | All rights reserved

What are cut sets?

- What are Cut Sets?
  - Cut sets are the combinations of minor failures that result in the overall failure of the system.



Settings

Diagram: FaultTree1
Sort By: Reliability (values in parentheses)
Time: 100.000000
Show All: Yes

Minimal Cut Sets

Set 1 (1 block) (0.968872) : Failure Mode 1

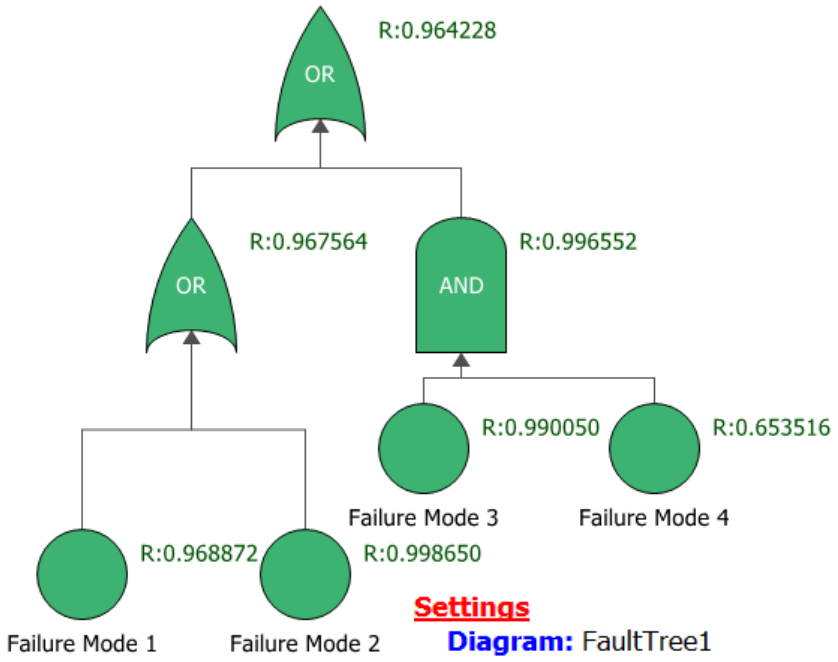
Set 2 (2 blocks) (0.996552) : Failure Mode 3, Failure Mode 4

Set 3 (1 block) (0.998650) : Failure Mode 2

www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved
CONFIDENTIAL - EXTERNAL

Why do Cut Sets matter?

- Cut Sets provide the ability to show the different combinations of potential faults which lead to a system failure.
- Of note: A common mistake with Fault Trees and FMEAs is not having a well-defined definition of failure.
- Tips to avoid this pitfall:
  - Provide a standard of performance that ties into your requirements.
  - Make sure each failure criteria aligns with not meeting your specified requirements



Settings

Diagram: FaultTree1
Sort By: Reliability (values in parentheses)
Time: 100.000000
Show All: Yes

Minimal Cut Sets

Set 1 (1 block) (0.968872) : Failure Mode 1

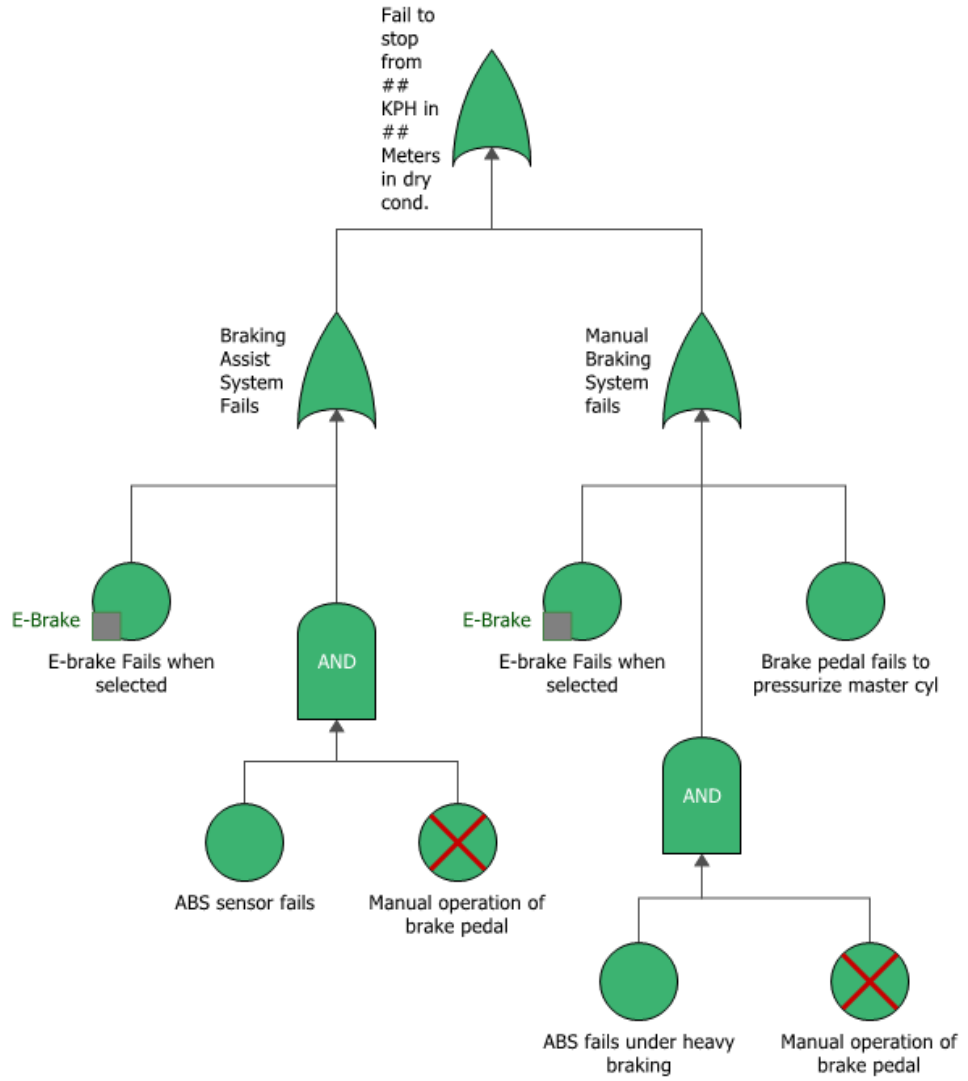
Set 2 (2 blocks) (0.996552) : Failure Mode 3, Failure Mode 4

Set 3 (1 block) (0.998650) : Failure Mode 2

www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved
CONFIDENTIAL - EXTERNAL

A simplified example:

- In this example, we will take a look at the simplified braking system from a vehicle.
- We'll make note that the general requirement of "stop from specified speed in specified distance in specified conditions" satisfies our standard of performance.
- Additionally, just as in FMEAs certain assumptions will be made (human factors) and others will need to be called out (specific failure scenarios).



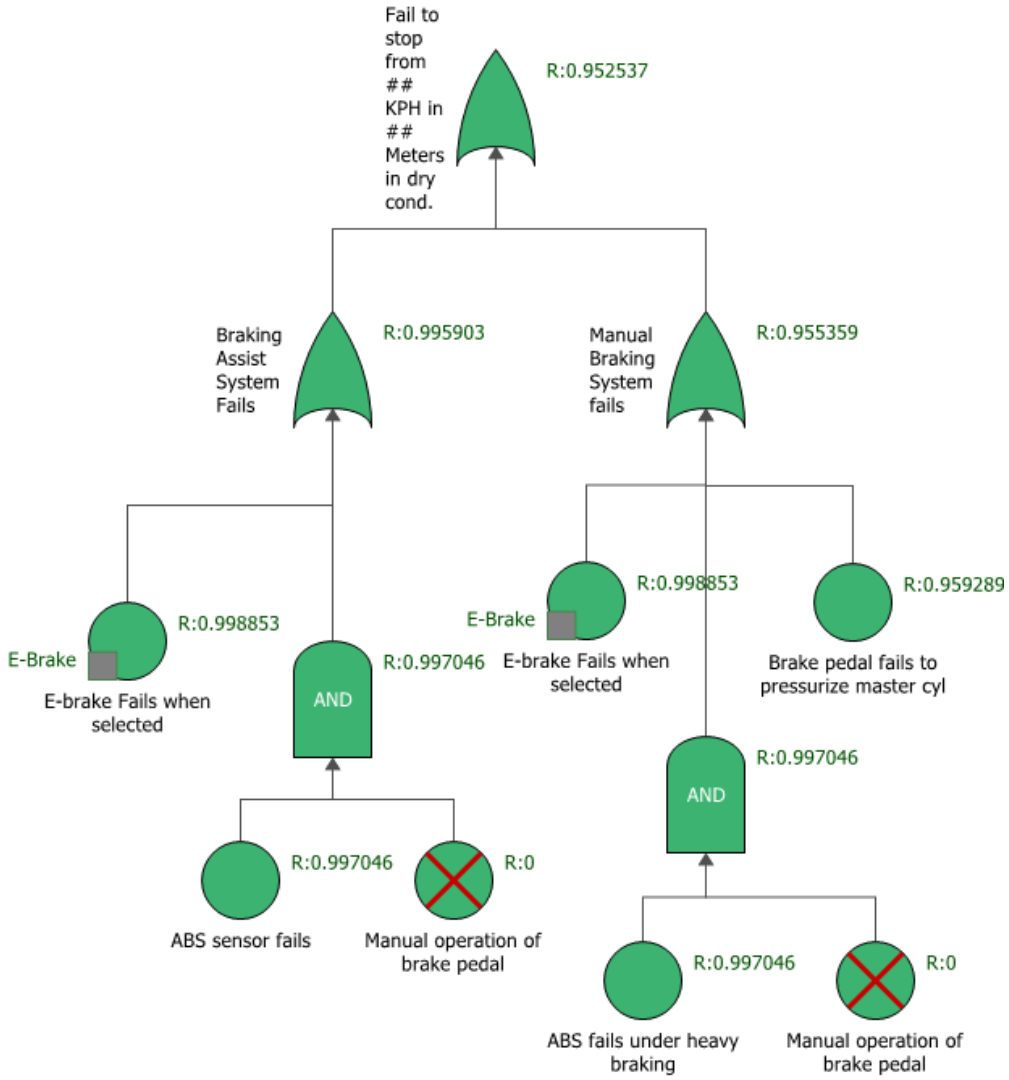
www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Initial Calculation – 30,000 Km

- Taking into account our assumptions with regard to the failure behavior of our systems, and calculating to 30,000 Km we observe that there is a 95.2% reliability value for the braking system to work as expected at 30,000 Km.

- We similarly observe that with the systems as presently specified that the master cylinder is the primary contributor to this result, as all other systems are greater than 99.8% reliability.



www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Cut Sets

- From the cut sets we can then show these results in a more tabular format.

Settings

Diagram: Baseline Scenario
Sort By: Reliability (values in parentheses)
Time: 30000.000000
Show All: Yes

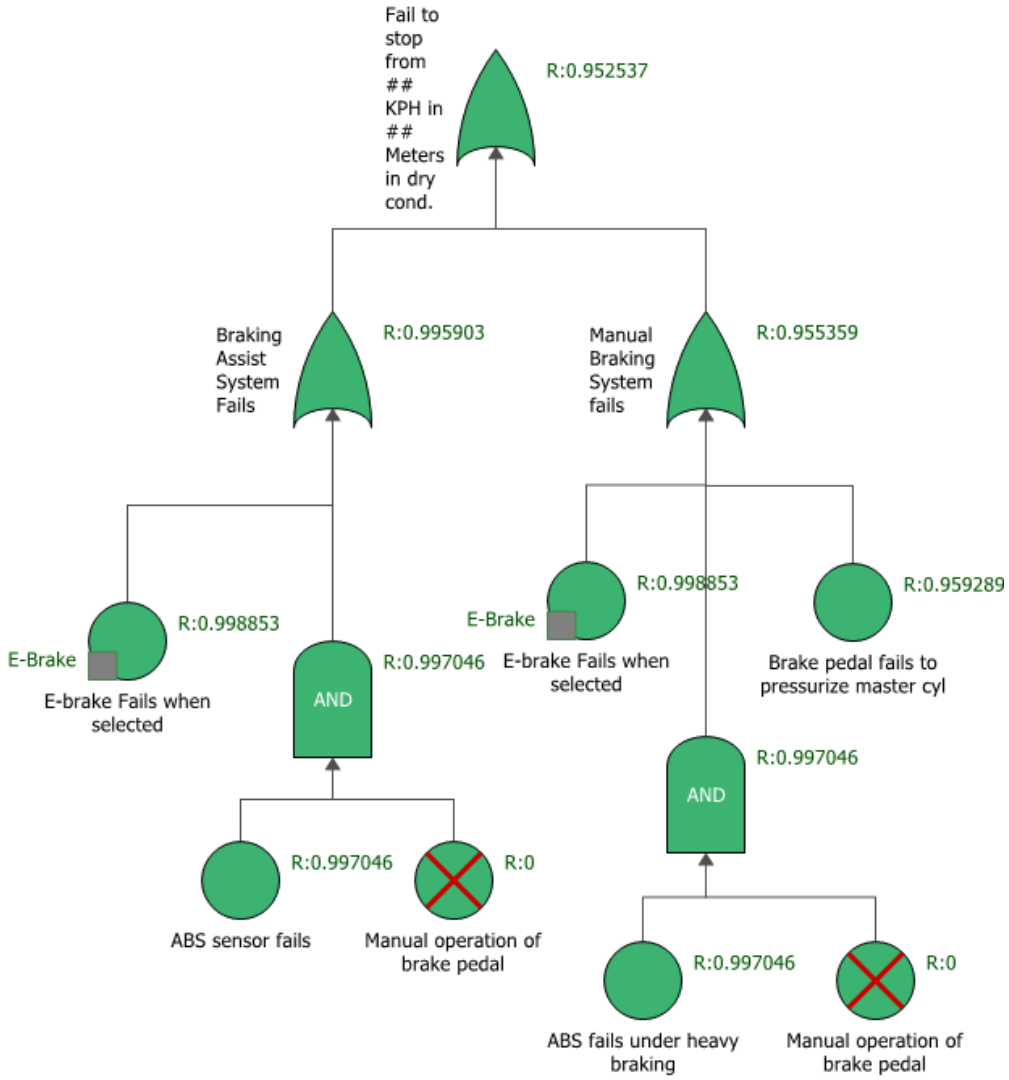
Minimal Cut Sets

Set 1 (1 block) (0.959289) : Brake pedal fails to pressurize master cyl

Set 2 (2 blocks) (0.997046) : Manual operation of brake pedal, ABS fails under heavy braking

Set 3 (2 blocks) (0.997046) : ABS sensor fails , Manual operation of brake pedal

Set 4 (1 block) (0.998853) : E-brake Fails when selected



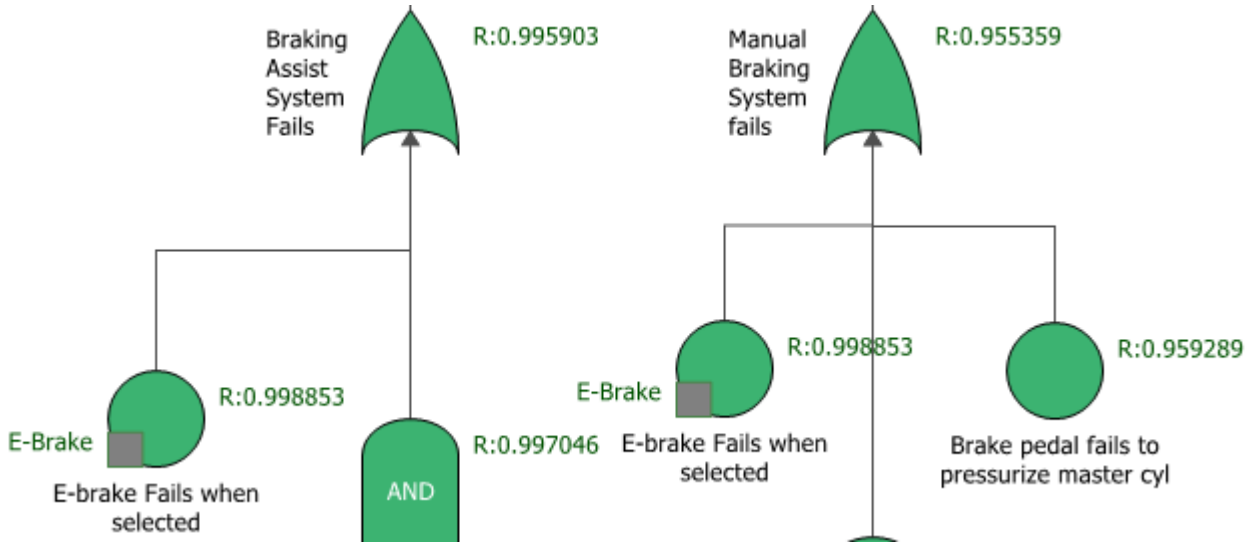
www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Common Cause Analysis

- You might notice that there are two blocks here with the same description and a gray square on them. In the application used to create these diagrams this indicates that they belong to a group of linked events within the diagram.

- These typically represent an event which exists in more than one branch, and so if that event occurs in one branch, it is assumed to have occurred in all other branches where it is linked.

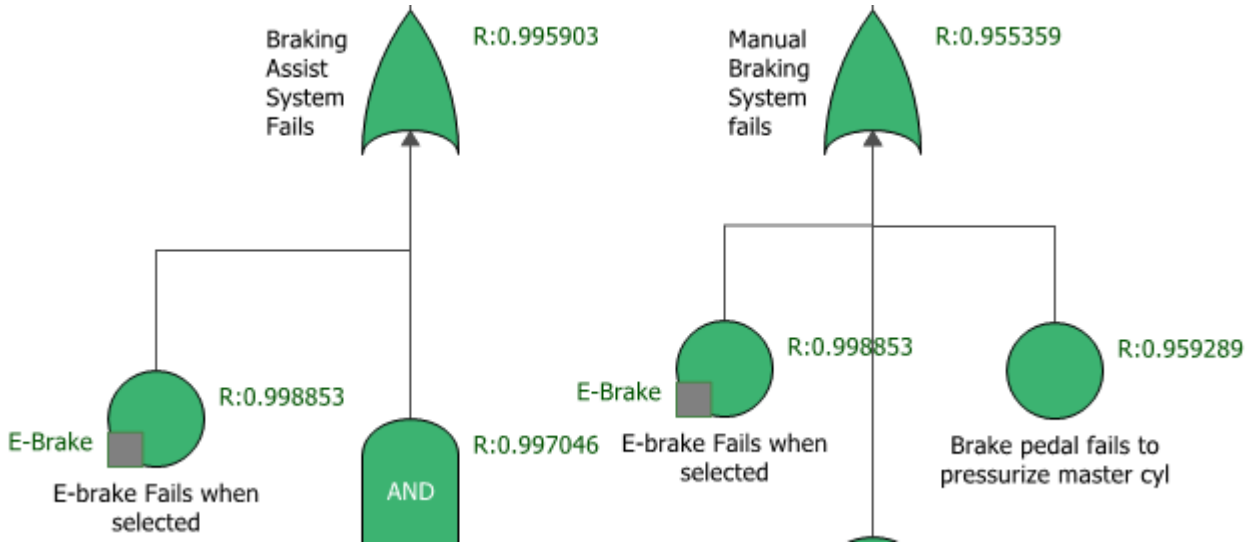


www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Common Cause Analysis

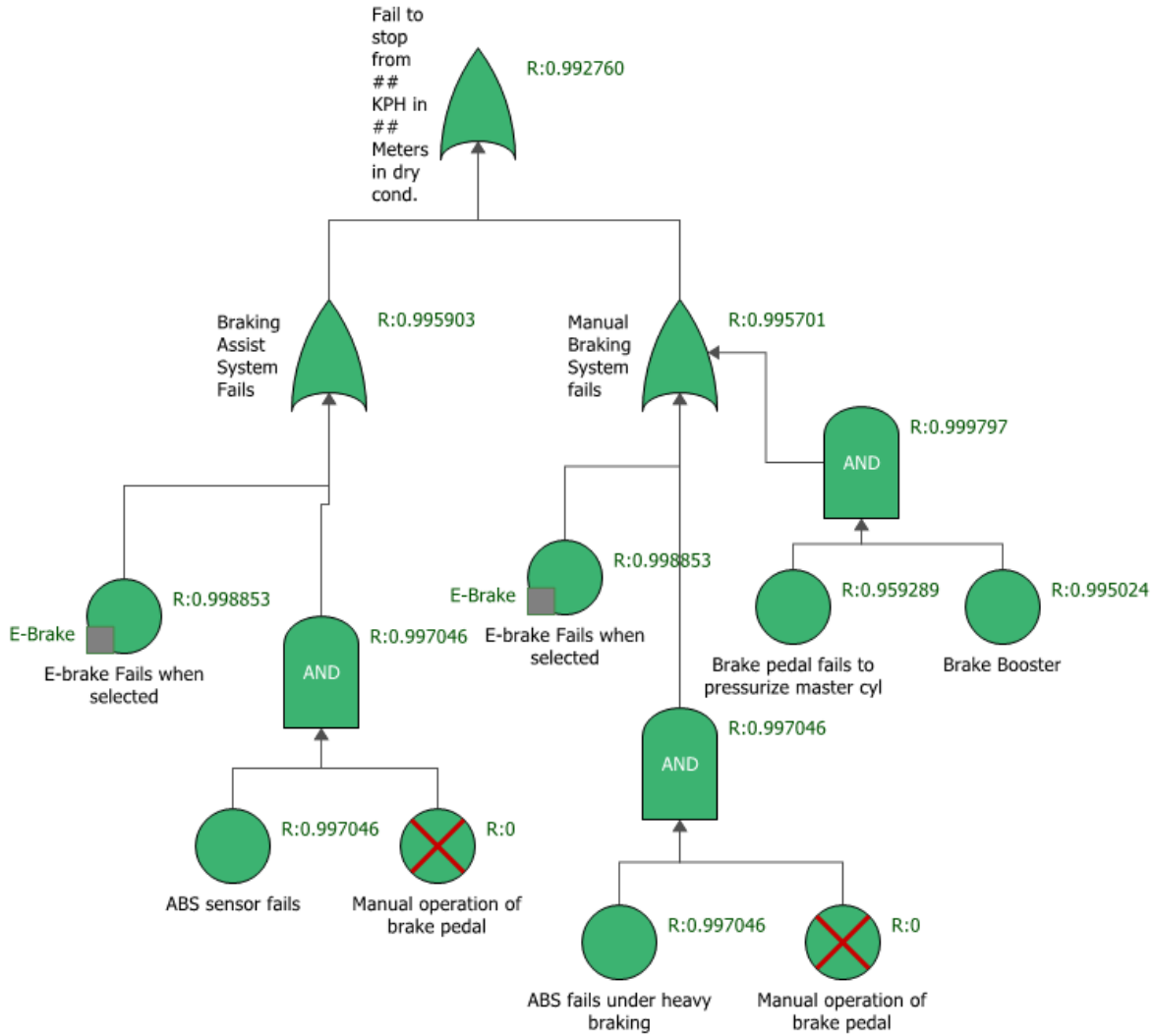
- Common causes are used to represent:
  - Configurations where the same component or event is necessary to be represented in multiple branches.
  - Configurations where the underlying event is inextricably linked between two separate branches.



www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved
CONFIDENTIAL - EXTERNAL

Adding redundancy to the system

- AND gates in fault trees are used to show where there is a redundant mechanism or component.
  - In this scenario we have added a brake booster to the pedal / master cylinder system and assume that with this addition that we need both to fail to send the necessary pressure to engage the brakes.
  - Note the change in overall reliability and in the branch in question.



www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Reviewing the results

- Reviewing the cut sets after adding redundancy we see that each element in this system is now improved to a level which, with routine recommended maintenance, can contribute into an overall reliable system.

- Note: the reliability of subsystems being as high as possible is necessary for the overall reliability of the top level system.

Settings

Diagram: Baseline Scenario
Sort By: Reliability (values in parentheses)
Time: 30000.000000
Show All: Yes

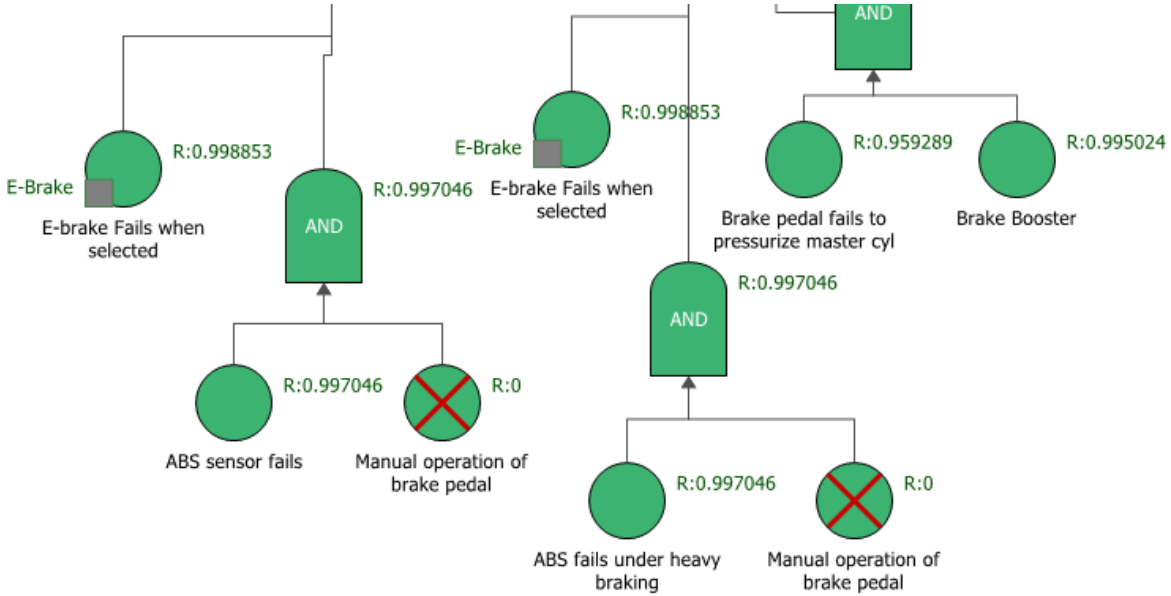
Minimal Cut Sets

Set 1 (2 blocks) (0.997046) : Manual operation of brake pedal, ABS fails under heavy braking

Set 2 (2 blocks) (0.997046) : ABS sensor fails , Manual operation of brake pedal

Set 3 (1 block) (0.998853) : E-brake Fails when selected

Set 4 (2 blocks) (0.999797) : Brake Booster, Brake pedal fails to pressurize master cyl



www.hbkworld.com | © HBK - Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Summary

1. The assumptions are the same in the FMEA as that assumed for the FTA and external factors contribute to the knowledge and understanding gained throughout the analyses.

2. Demonstrated that Safety Engineering can influence the Design intent and vice versa.

www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

CONFIDENTIAL - EXTERNAL

Thank You

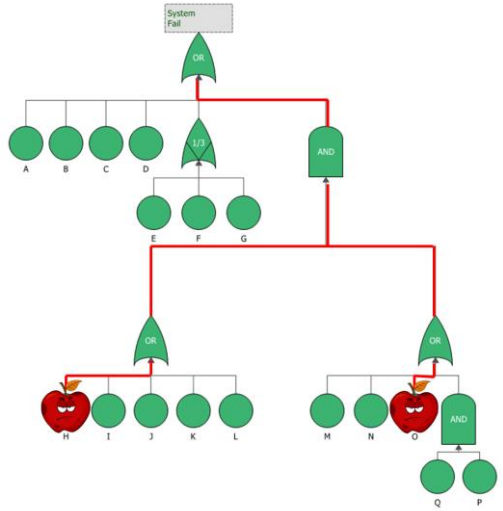
Presenters:

- **Chris Wynn-Jones,** *ReliaSoft Application Engineer*
- **Sam Eisenberg,** *Product Manager - ReliaSoft*

www.hbkworld.com | © HBK – Hottinger, Brüel & Kjær | All rights reserved

HBK Technology Days – Virtual Seminar Series

Tuesday, November 22, 2022



Fault Tree Analysis – the Critical Path! – Uncover your Unreliability Drivers

Presented by Chris Wynn-Jones and Sam Eisenberg
Reliability Application Engineer & Product Manager, HBK ReliaSoft Products

UNRESTRICTED