University of Nottingham
UK | CHINA | MALAYSIA

Lloyd's Register Foundation

Next Generation Prediction Methodologies and Tools for System Safety Analysis

Professor John Andrews

PRIMA VERA Colloquium
Wednesday 7th April

John Andrews - CV

- BSc – Industrial Mathematics
- PhD – 'A Finite Element Study of the Stress Distribution in Epicyclic Gears'

British Gas – Senior Scientist/Engineer in Risk Assessment
Midlands Research Station

Loughborough University
- Mathematical Sciences Department – Professor of Mathematical Engineering
- Aeronautical and Automotive Engineering – Professor of Risk Assessment

University of Nottingham (2009)
– Royal Academy of Engineering & Network Rail Professor of Infrastructure Asset Management
– Head of the Resilience Engineering Research Group
  - Mechanical , Materials and Manufacturing Engineering

Contents

Next Generation of Prediction Methodologies and Tools for Safety System Analysis Review of the Current Methodologies

- Project Overview
- Current Approaches
  - Fault Tree Analysis
  - Event Tree Analysis
- Alternative Approaches
  - Binary Decision Diagrams
  - Petri Net models
  - Integration of the methods
- Case Study
- Summary /Conclusions

Lloyd's Register Foundation

University of Nottingham
UK | CHINA | MALAYSIA

Project Overview

Background & Objectives

Background

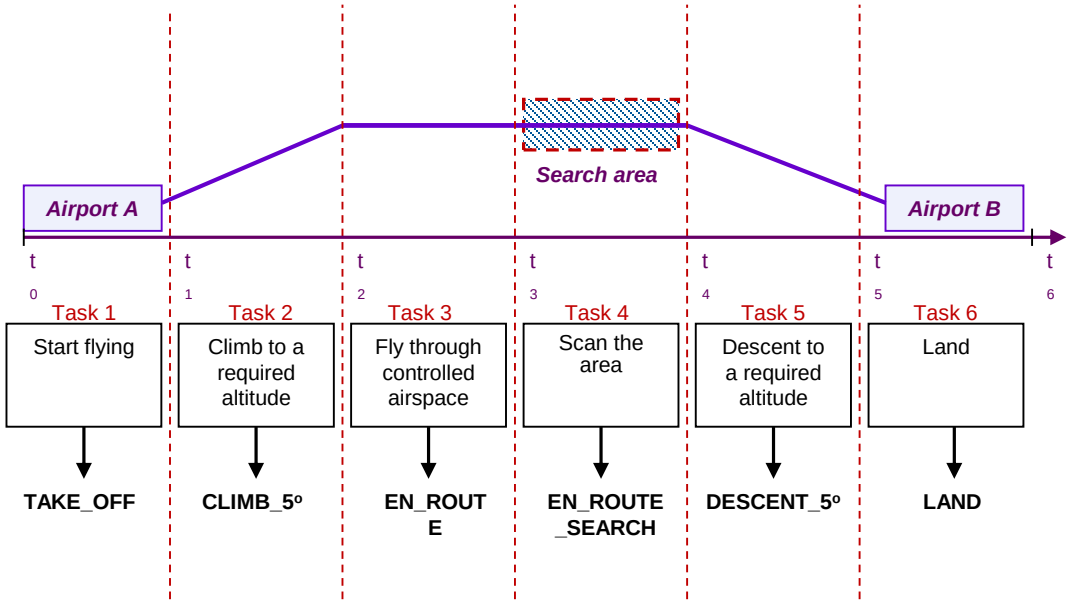
- Current Risk Assessment tools include: Fault Tree Analysis, Event tree Analysis
- The foundations of methodologies for safety critical systems were established in the 1960/70s.
  - Research has made considerable advances in the capabilities of analytical techniques since then.
  - Technology has advanced and system designs, their operating conditions and maintenance strategies are now significantly different to those of the 1970s.

Objectives

- This project challenge - develop a single, generic methodology appropriate to meet the demands of modern industrial systems.
- Retain as much of the current methodology features as possible:
  - to reduce the learning curve for practitioners
  - increase the chances of acceptance.

Summary

- 4 phases
  - Phase 1 – extend the capabilities of Fault Tree & Event tree Analysis
  - Phase 2 – extend the capabilities of phased mission analysis
  - Phase 3 – add dynamic capabilities to the modelling
  - Phase 4 – integrate stochastic models of the system failures with discrete physical models (eg core damage events in nuclear reactors)



University of Nottingham
UK | CHINA | MALAYSIA

Industrial Partners

Network Rail

HIGH SPEED 1

HS2

RSSB

First

NetworkRail High Speed Ltd.

DAE

IGCAR

BARC

ROLLS ROYCE

BAE SYSTEMS

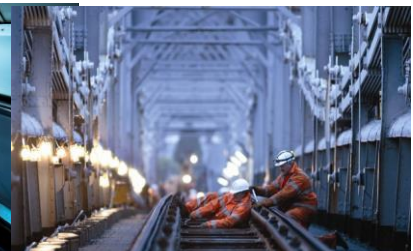
Lloyd's Register Foundation

Lloyd's Register







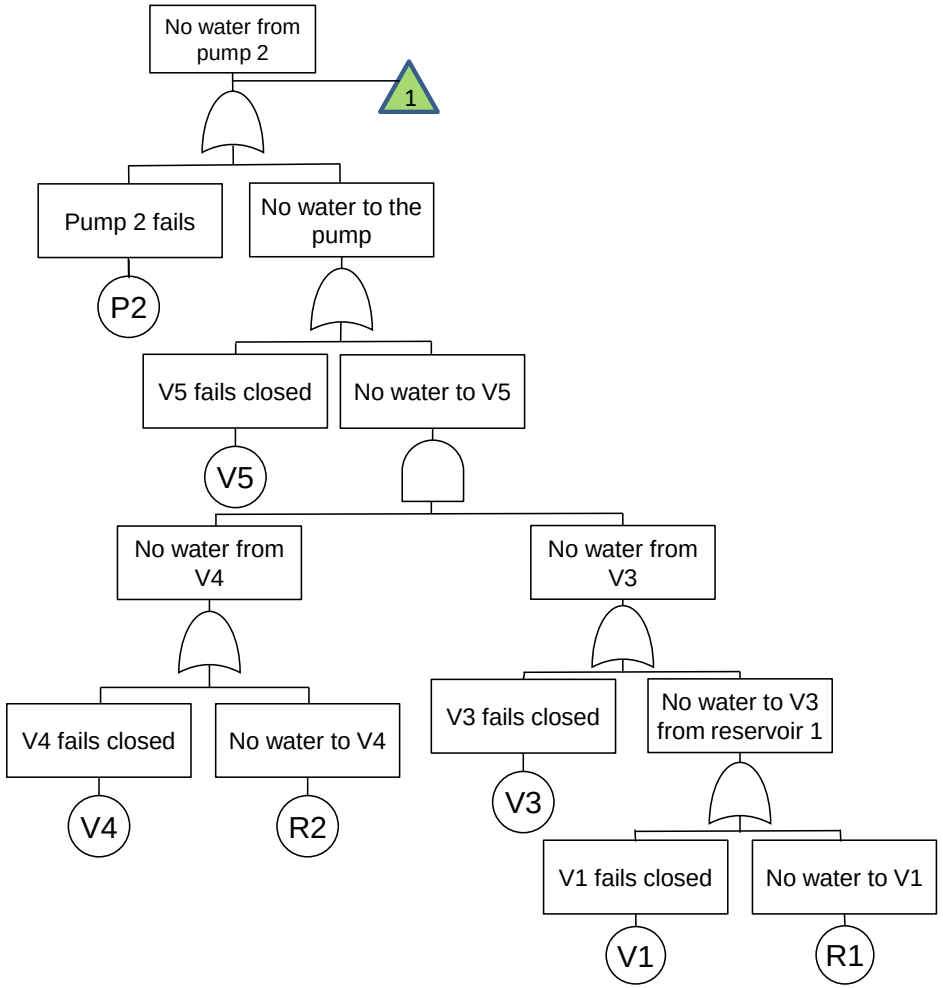



University of
Nottingham
UK | CHINA | MALAYSIA
Current
Approaches
Event Tree Analysis / Fault Tree Analysis

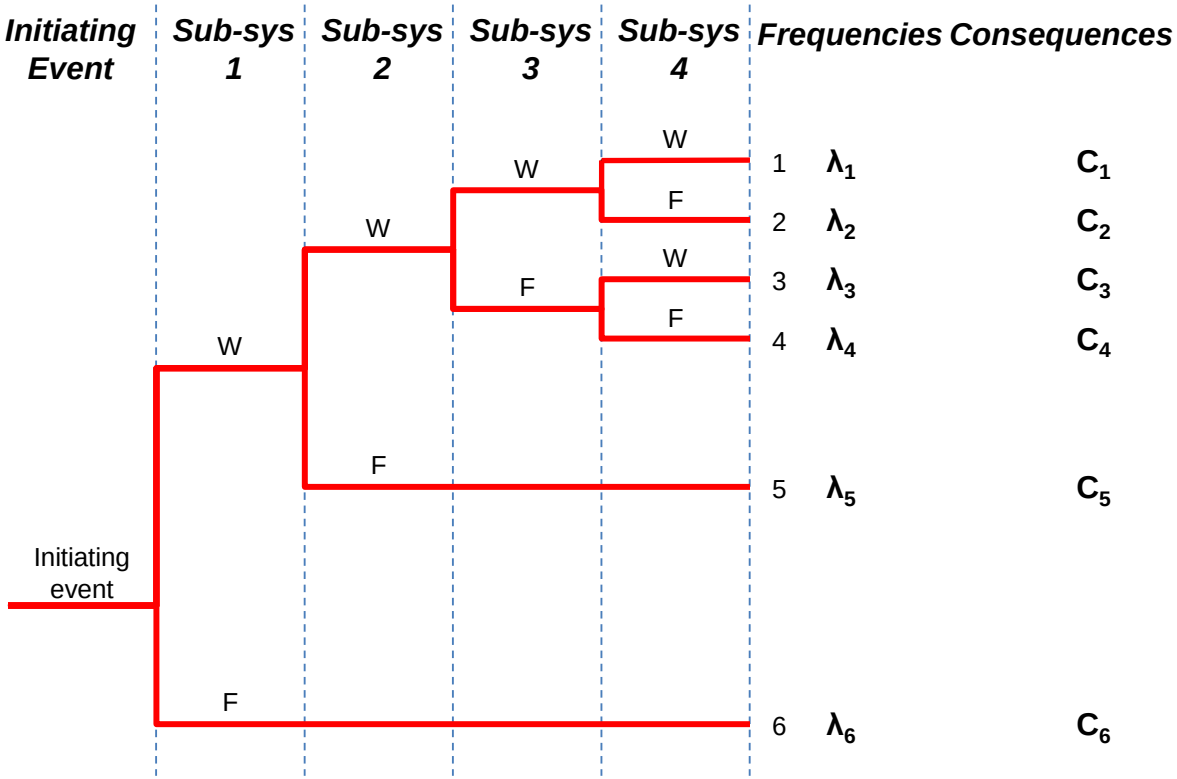
Traditional Approaches to Risk Modelling

Integrated Fault Tree Analysis / Event Tree Analysis Approach

Fault Tree Analysis

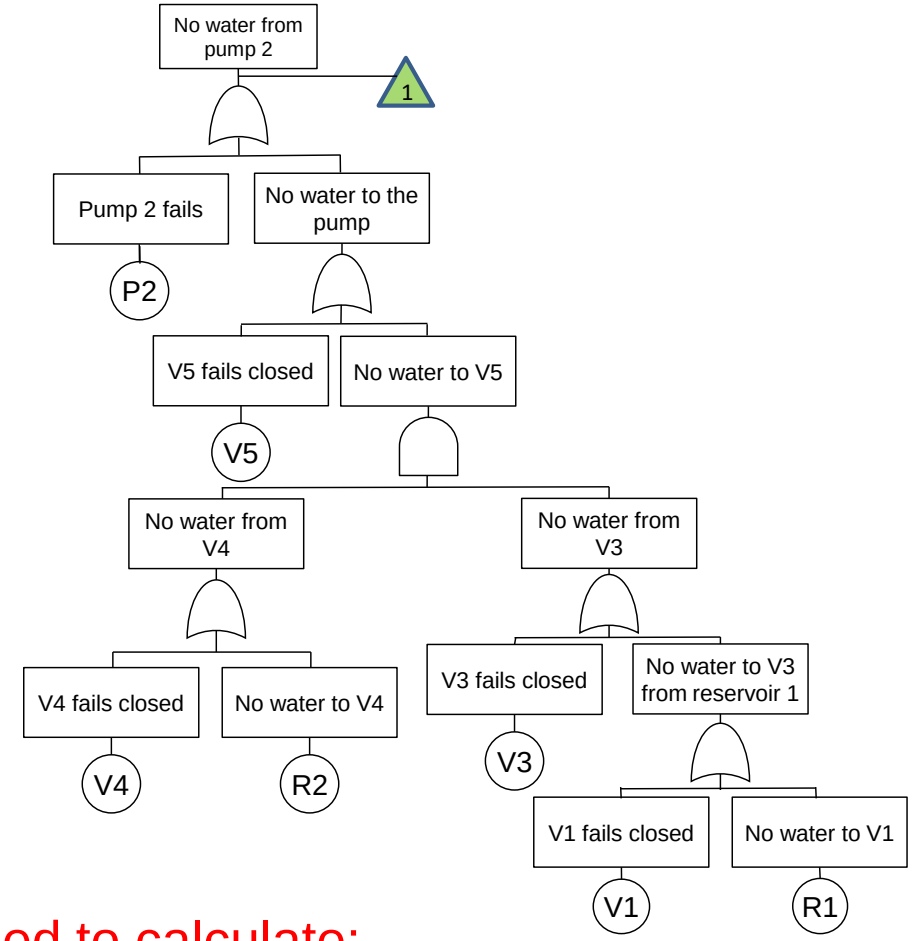


Event Tree Analysis



$$Risk = \sum_{i=1}^{6} \lambda_i C_i$$

Fault Tree Analysis



Used to calculate:

- Frequency of the initiating event
- Unavailability of enablers (responding safety systems)

Method Assumptions / Limitations

- Component failures are independent
- Constant failure rates

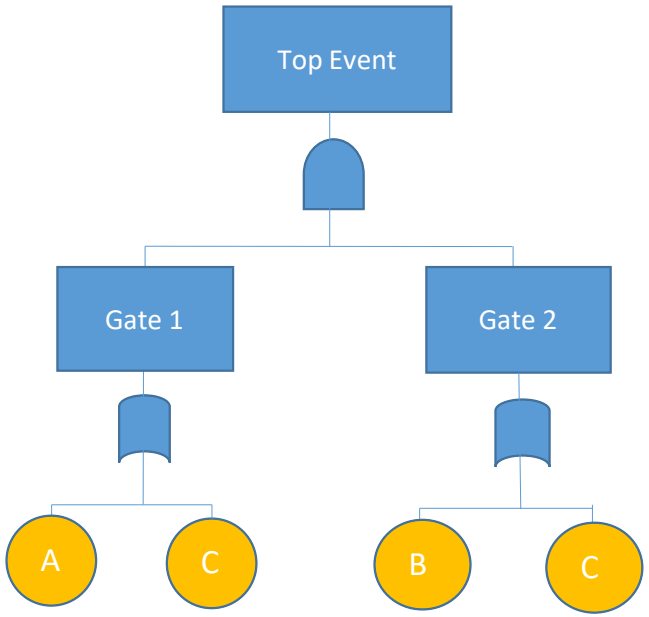
Component failure models

- Limited maintenance process detail
  - No Repair: $Q(t) = F(t) = 1 - e^{-\lambda t}$
  - Revealed: $Q(t) = \frac{\lambda}{\lambda + \nu}\left(1 - e^{-(\lambda+\nu)t}\right)$
  - Unrevealed: $Q_{AV} = \lambda\left(\frac{\theta}{2} + \tau\right)$

PROJECT AIMS

- Incorporate non-constant failure rates
- Incorporate dependent events
- Incorporate highly complex maintenance strategies

Fault Tree Analysis – Top Event Probability



$$TOP = (A + C).(B + C)$$

\+ OR

. AND

Minimal Cut Sets: {A, B}, {C}

Exact

$$Q_{SYS} = q_A\, q_B + q_C - q_A\, q_B\, q_C$$

Approximate

$$Q_{SYS} \leq 1 - (1 - q_A\, q_B)(1 - q_C)$$

Inclusion – exclusion expansion

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

Minimal Cut Set Upper Bound

$$Q_{SYS} \leq 1 - \prod_{i=1}^{N_c} (1 - P(C_i))$$

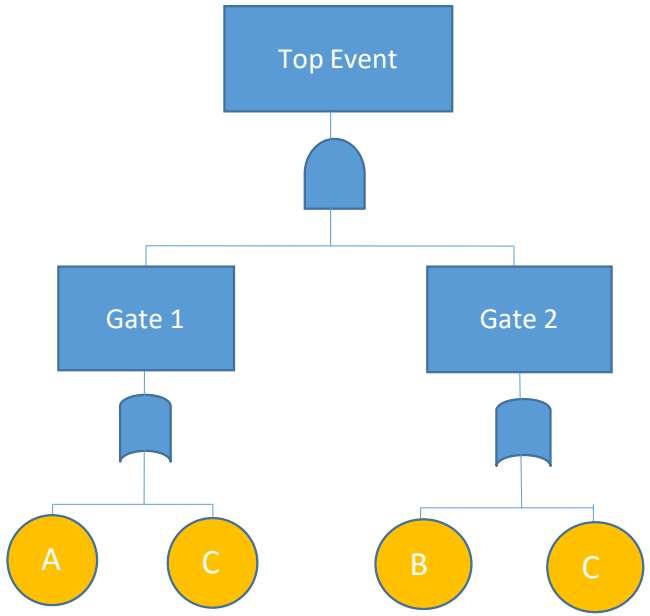
Initiator / Enabler events

Initiating Events: perturb system variables and place a demand on control / protection systems to respond

Enabling Events: are inactive control / protection systems which permit an initiating event to cause the top event

Critical System States: A critical state for a component i, is a state of the other components in the system such that the failure of component i causes the system to pass from the functioning to the failed state.

Fault Tree Analysis – failure intensity



Initiating events A, C

$$Q_{SYS} = q_A\, q_B + q_C - q_A\, q_B\, q_C$$

$$TOP = (\boldsymbol{A} + \boldsymbol{C}).(B + C)$$

+ OR

. AND

Minimal Cut Sets: {A, B}, {C}

Criticality Function for the initiators:

$$G_i(\boldsymbol{q}) = \frac{\partial Q_{SYS}}{\partial q_i}$$

$$G_A(\boldsymbol{q}) = q_B - q_B\, q_C = q_B(1 - q_C)$$

$$G_C(\boldsymbol{q}) = 1 - q_A\, q_B$$

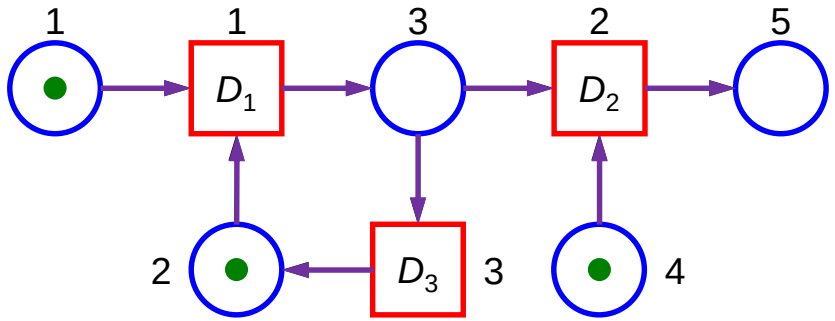
$$w_{SYS}(t) = \sum_{\substack{i \\ initiators}} G_i(\boldsymbol{q}).w_i\,(t)$$

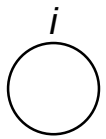
University of Nottingham
UK | CHINA | MALAYSIA

Alternative Methodologies

Binary Decision Diagrams / Petri Nets / Markov Methods

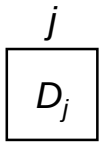
Petri Net Basics and Definitions





Places, p_i

- Marked with tokens



Transitions, t_j

- Time delay D_j determines token movement.
- Type:
  - immediate if $D_j = 0$
  - timed if $D_j \neq 0$

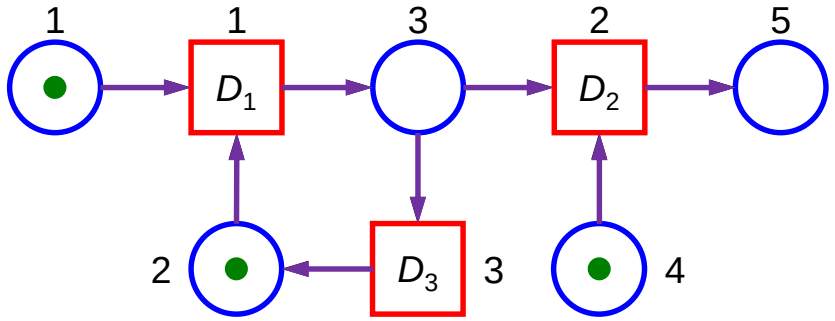
Edges

- From place to transition or transition to place.

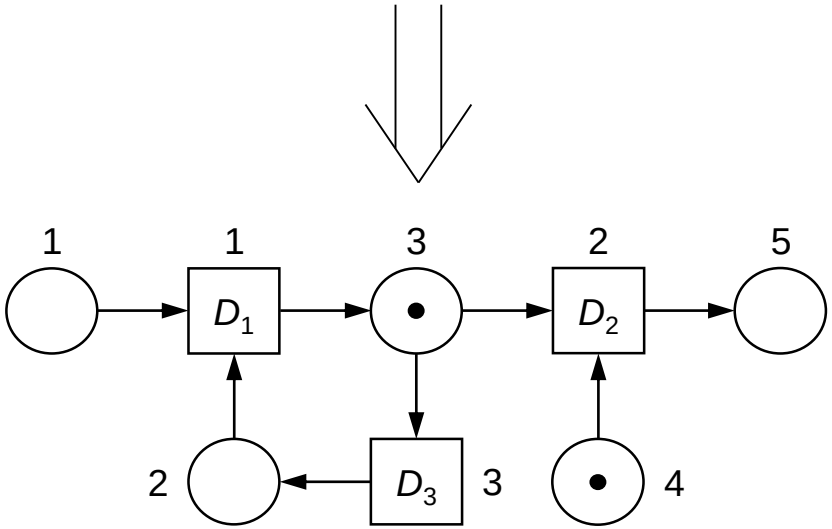
- Movement of tokens governed by the firing rule...

Petri Net Modelling

- If all input places of a transition are marked by at least one token then this transition is called **enabled**.

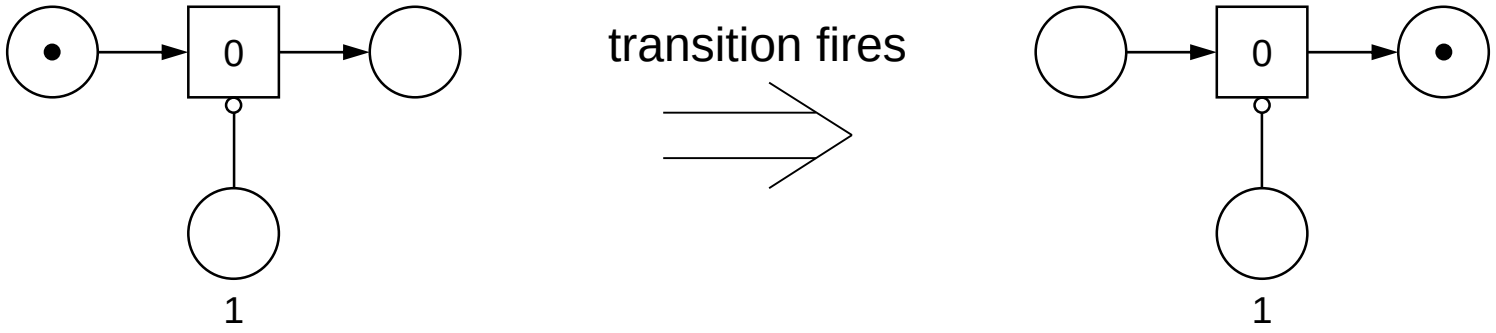


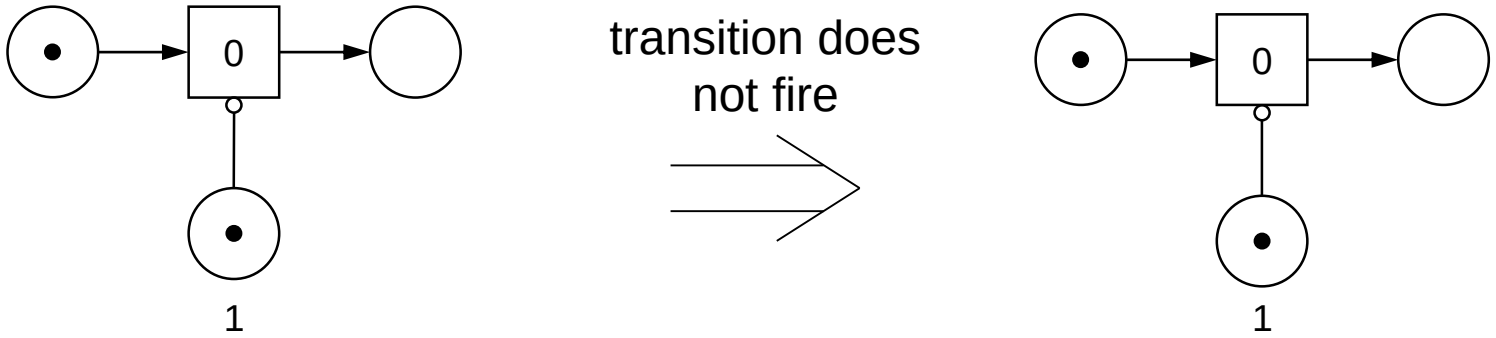
- After a delay $D \geq 0$ the transition **fires**. The firing removes one token from each of its input places and adds one token to each of its output places.



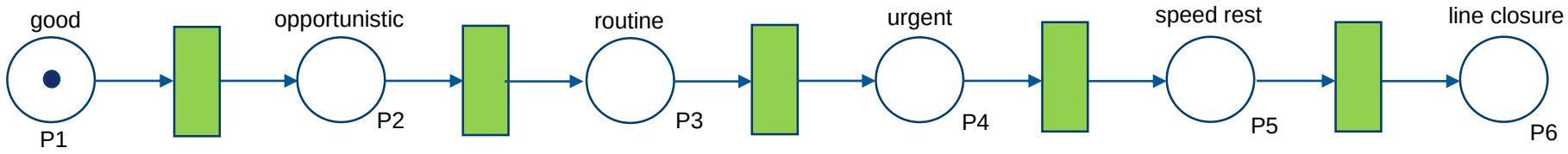
Inhibit Edges

- Blocks a stream when the place it comes from is marked.

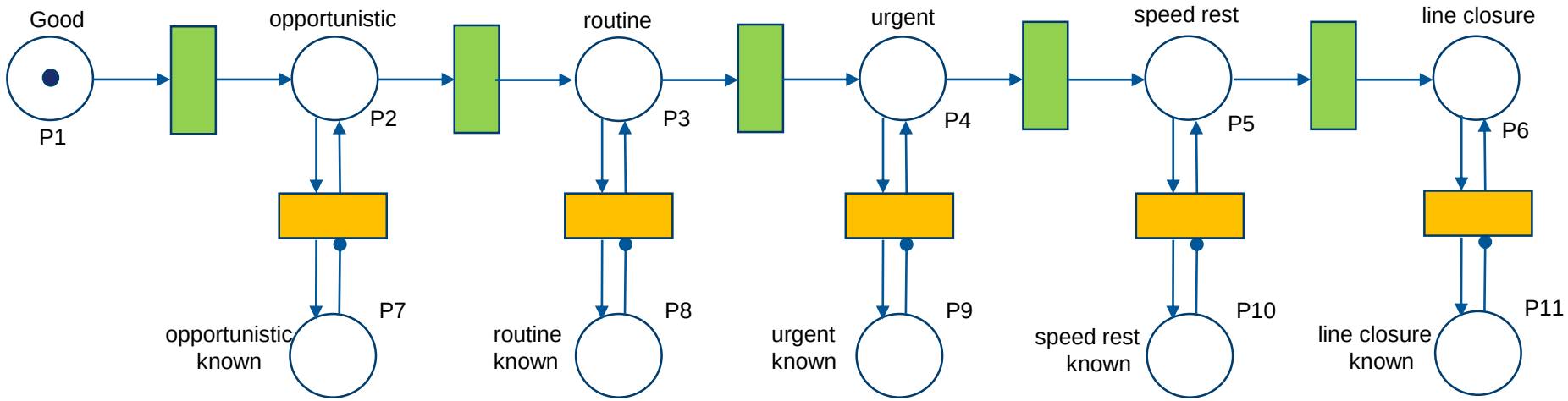




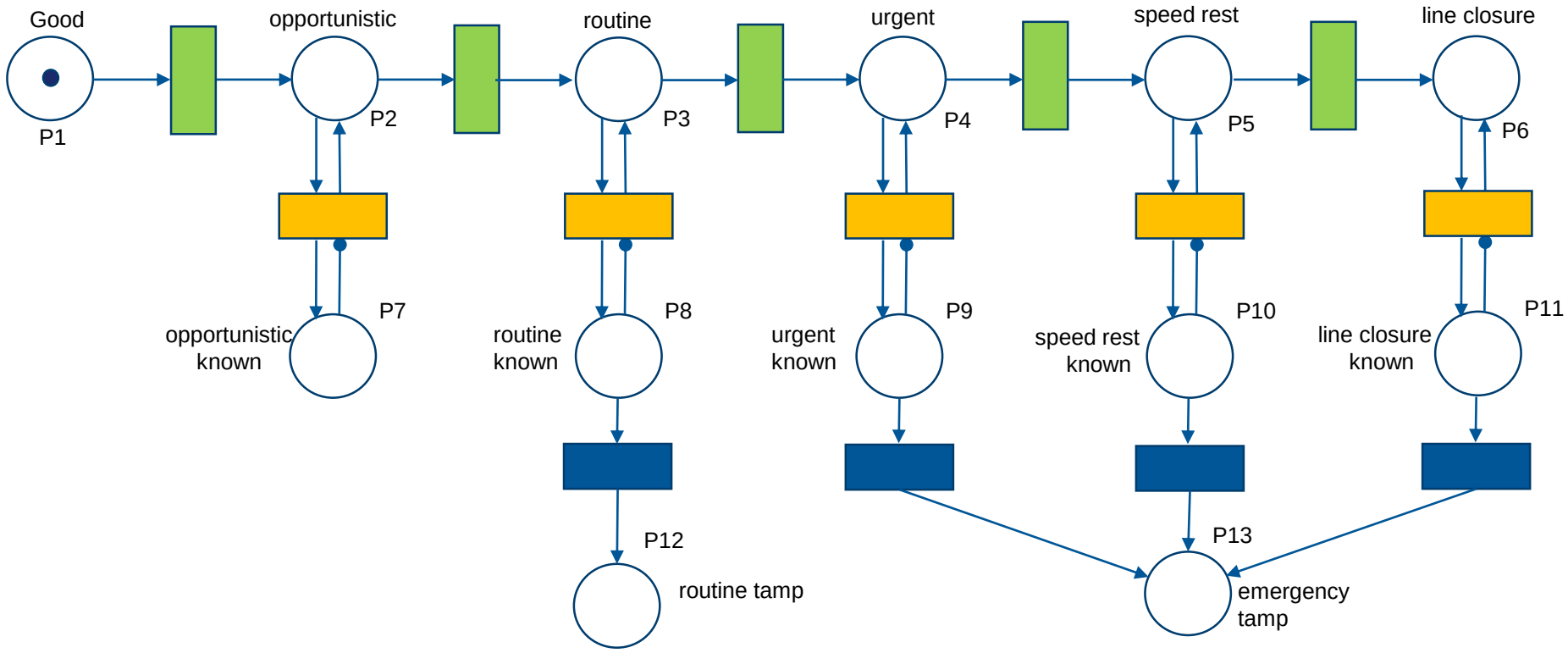
Example from the Railway Derailment Fault Tree



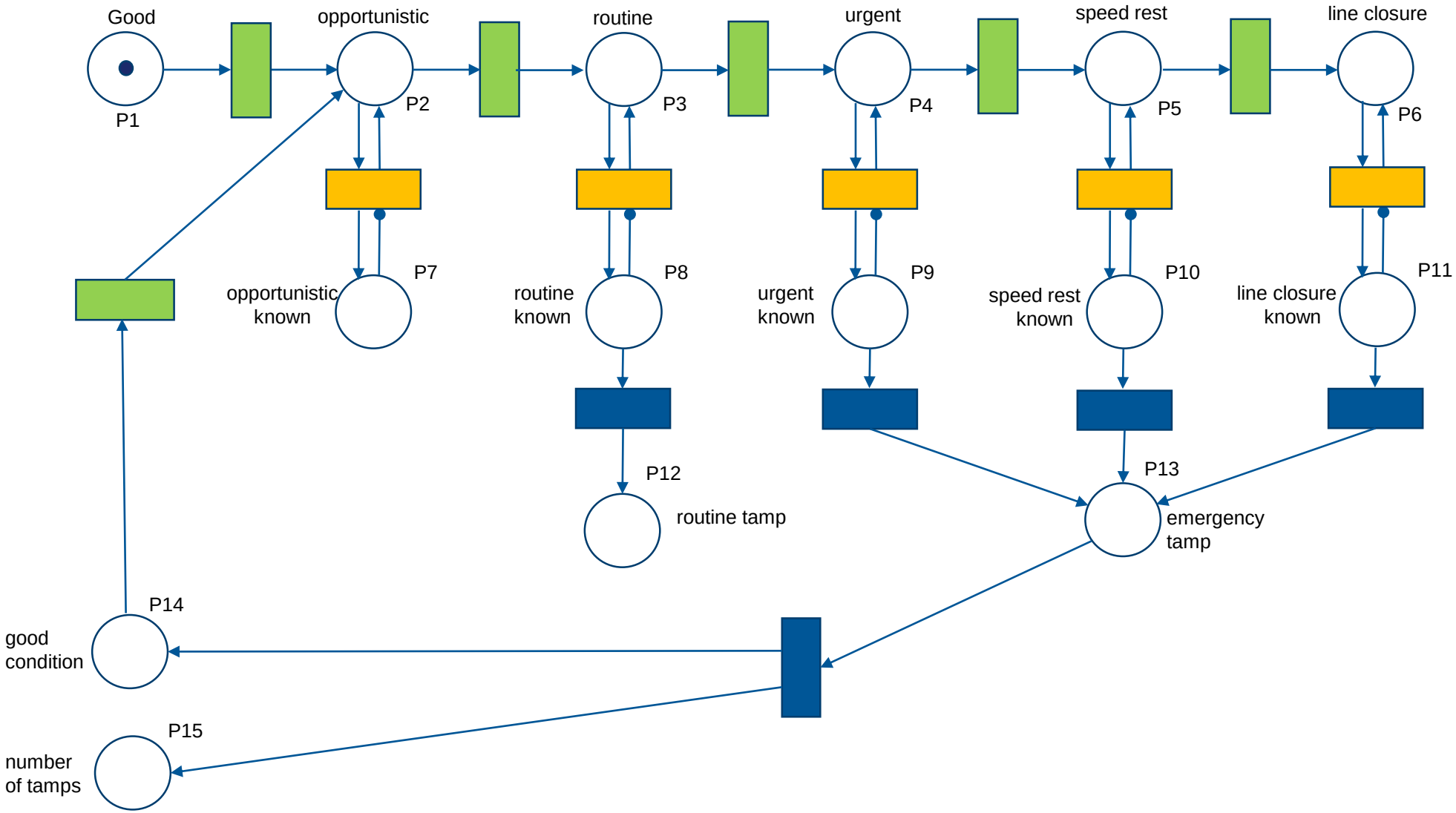
Degradation


Good
P1
opportunistic
P2
routine
P3
urgent
P4
speed rest
P5
line closure
P6
P7
opportunistic known
P8
routine known
P9
urgent known
P10
speed rest known
P11
line closure known

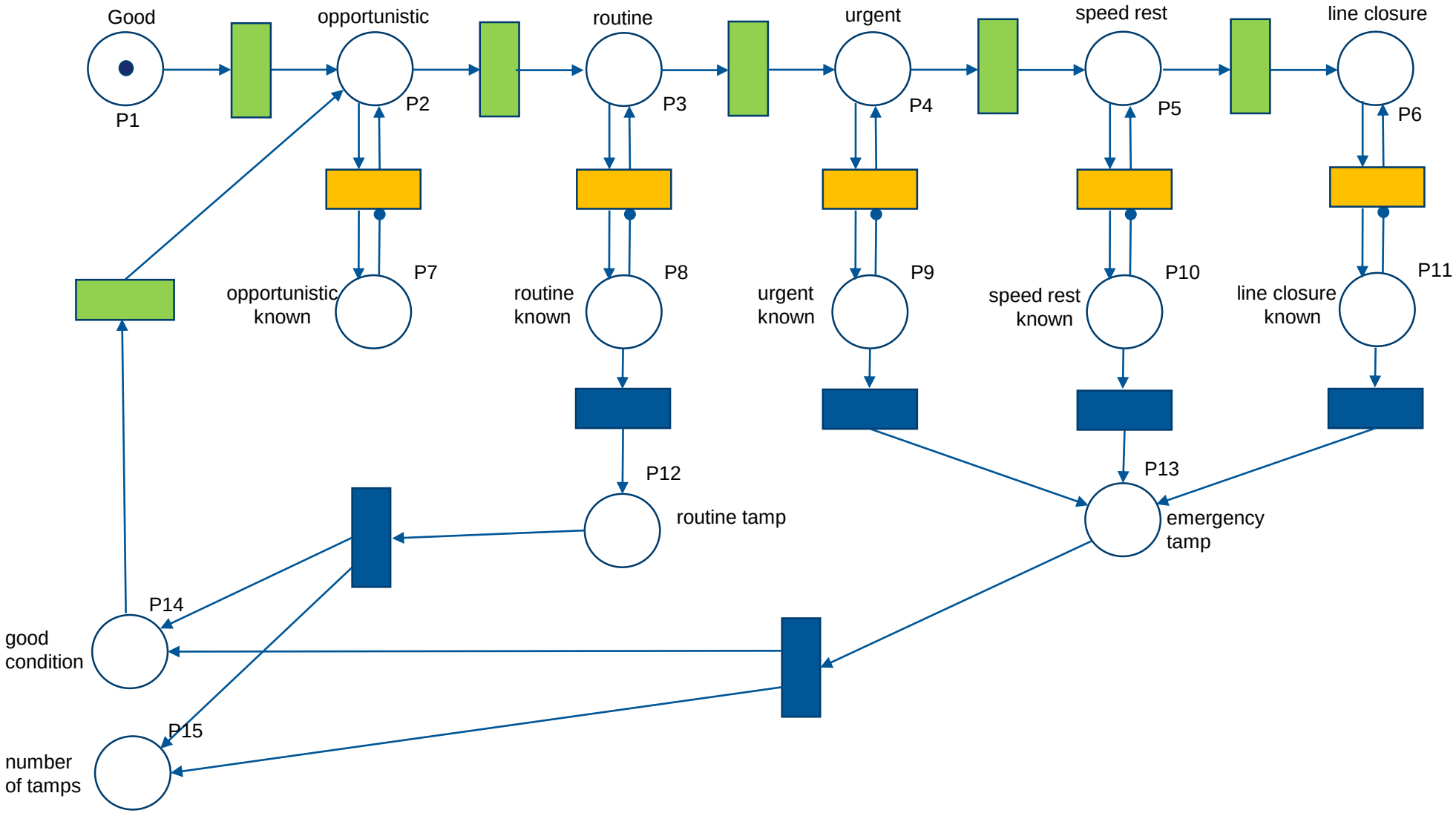
Inspection



Repair Options



Emergency Repair



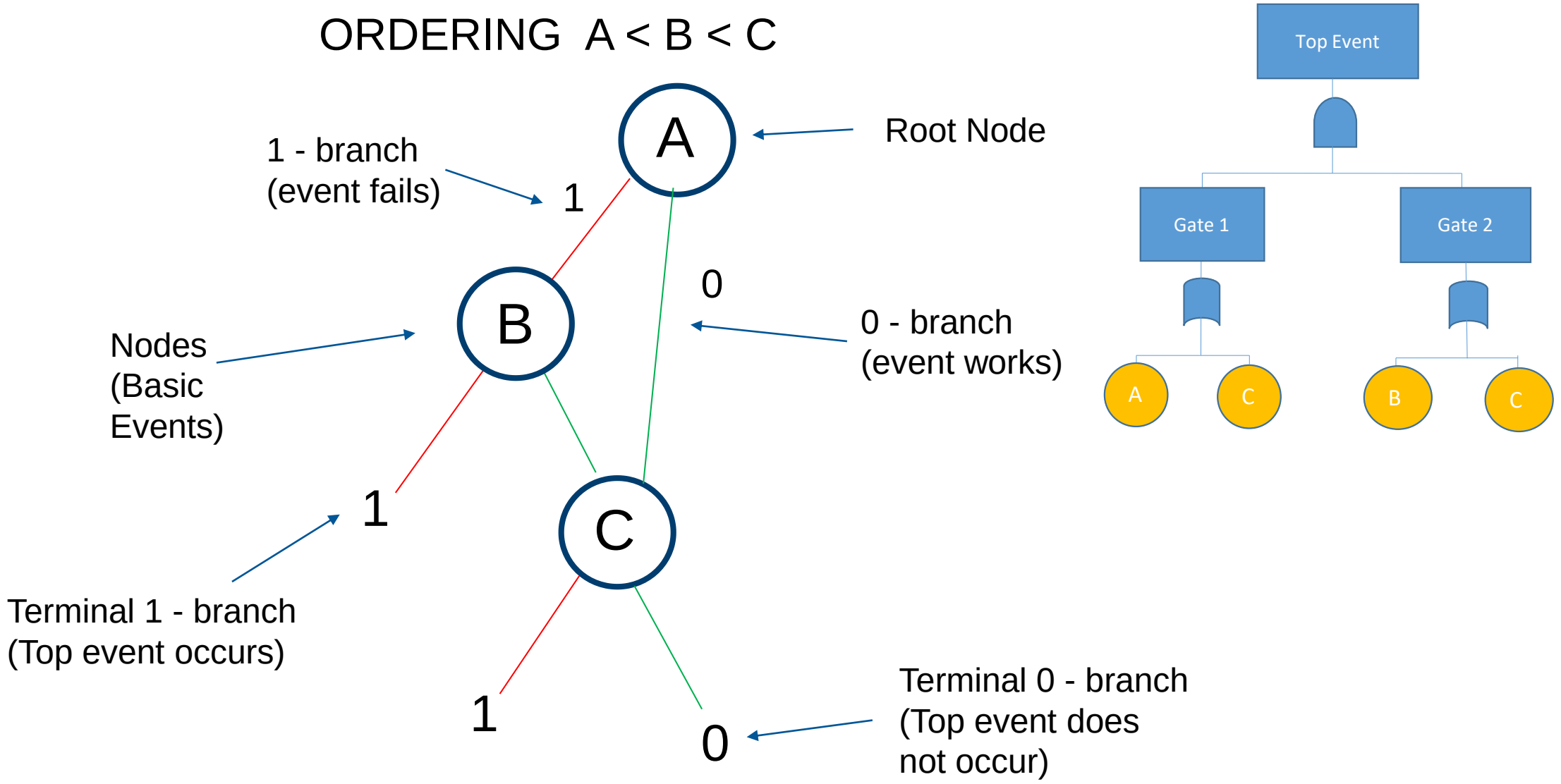
Routine Repair

University of Nottingham
UK | CHINA | MALAYSIA

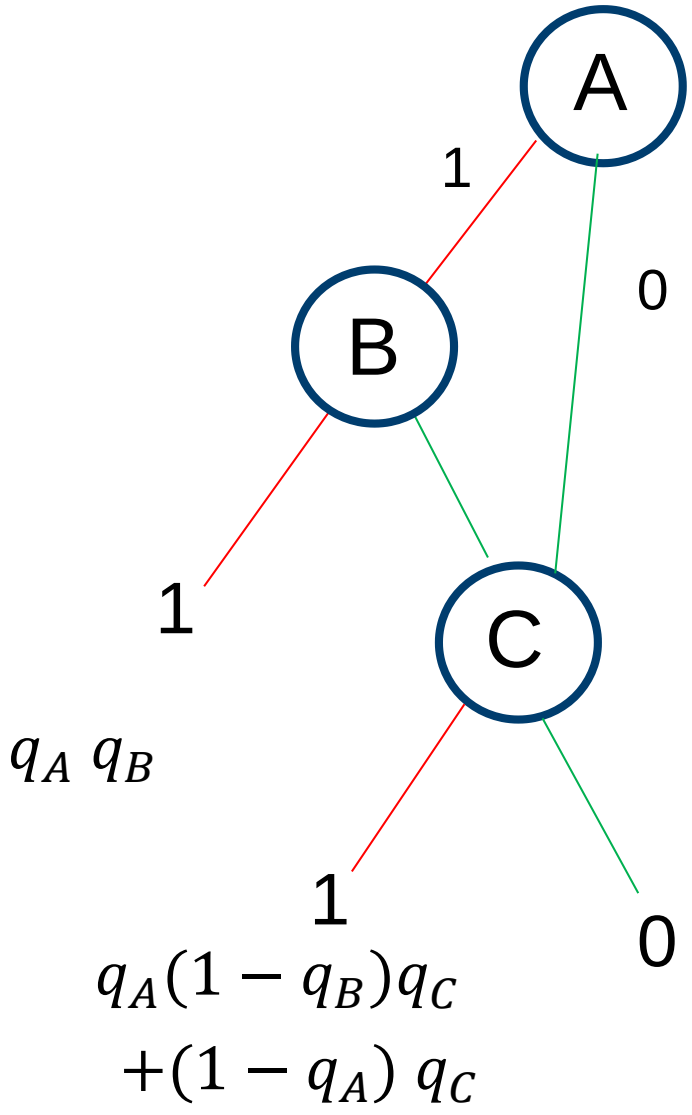
Model results – Asset Condition Performance

Condition	Condition Known?	Min Value	Average Value	Max Value	Comment
Good		92.66%	95.2%	97.31%	
Opportunistic		0.27%	0.42%	0.59%	
Routine		2.58%	3.11%	5.72%	
Urgent		1.12%	1.16%	1.18%	
Speed Restriction needed	Known	0.0%	0.005 %	0.018 %	
	Unknown	0.0%	0.043 %	0.056 %	Potential safety issue
Line Closure needed	Known	0.0%	0.005 %	0.018 %	
	Unknown	0.0%	0.057 %	0.07 %	Potential safety issue

Binary Decision Diagrams – Top Event Probability



Binary Decision Diagrams – Top Event Probability



$q_A\ q_B$

$q_A(1-q_B)q_C$

$+(1-q_A)\ q_C$

$$TOP = A.B + A.\bar{B}.C + \bar{A}.C$$

\+ OR

. AND

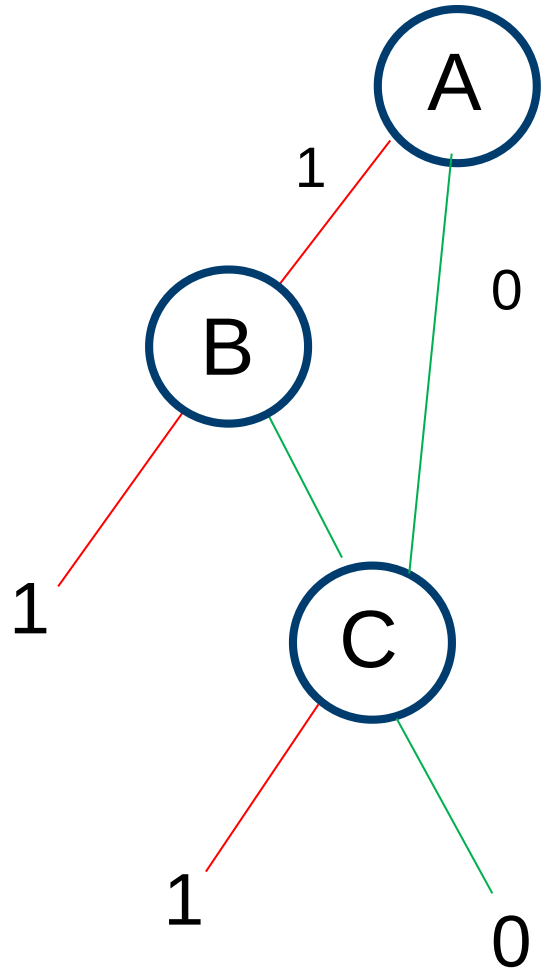
$$Q_{SYS} = q_A\ q_B + q_A(1-q_B)q_C + (1-q_A)\ q_C$$

$$= q_A\ q_B + q_C - q_A\ q_B\ q_C$$

- Exact
- Fast - Efficient – no need to get Min cut sets

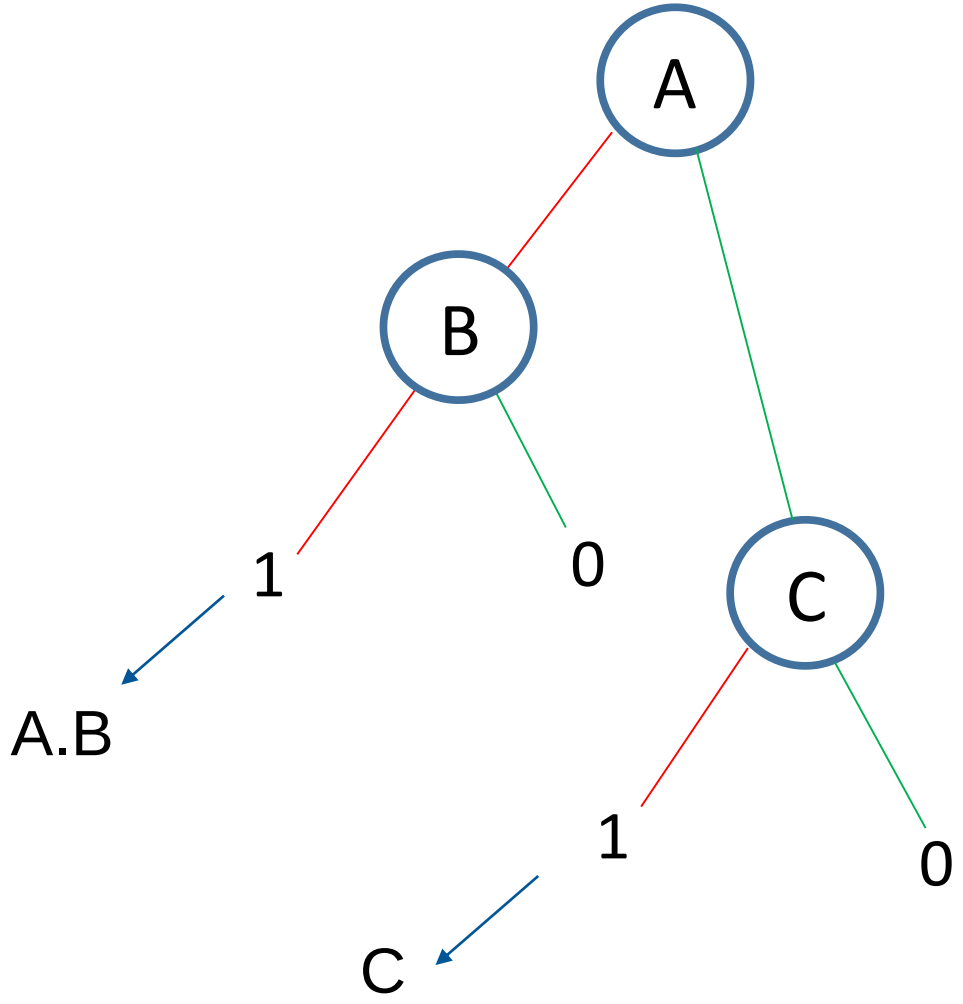
Binary Decision Diagrams – Minimal Cut Sets

Encodes Shannon's formula



Minimisation process

Encodes Minimal Cut Sets



Binary Decision Diagram – Top Event Frequency

$$w_{SYS}(t) = \sum_{\substack{i \\ initiators}} G_i(\boldsymbol{q}).w_i\,(t)$$

The Criticality Function, $G_i(q)$, is the probability that the system is in a critical state for component i such that the failure of component i causes system failure.

$w_i(t)$ is the failure intensity of component i.

$$G_i(\boldsymbol{q}) = \frac{\partial Q_{SYS}}{\partial q_i} = Q_{SYS}(1_i, \boldsymbol{q}) - Q_{SYS}(0_i, \boldsymbol{q})$$

$Q_{SYS}(1_i, \boldsymbol{q})$ probability that the system fails with component i failed

$Q_{SYS}(0_i, \boldsymbol{q})$ probability that the system fails with component i working

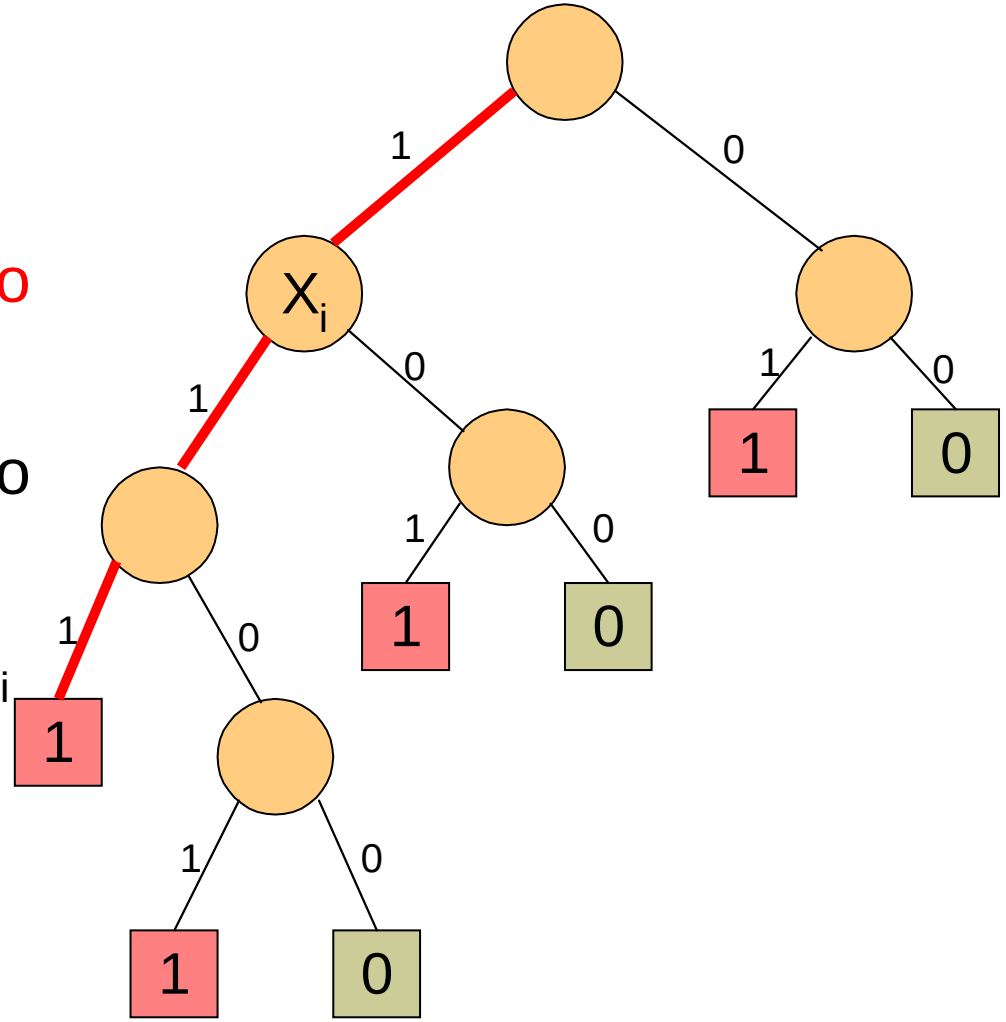
Note: the Criticality Function is also known as Birnbaum's Measure of importance

Criticality Function: Routes to a terminal-1

Criticality for X_i

Three Options:

1. paths through X_i on its 1-branch to a terminal-1
2. paths through X_i on its 0-branch to a terminal-1
3. paths which don't pass through X_i on way to a terminal-1

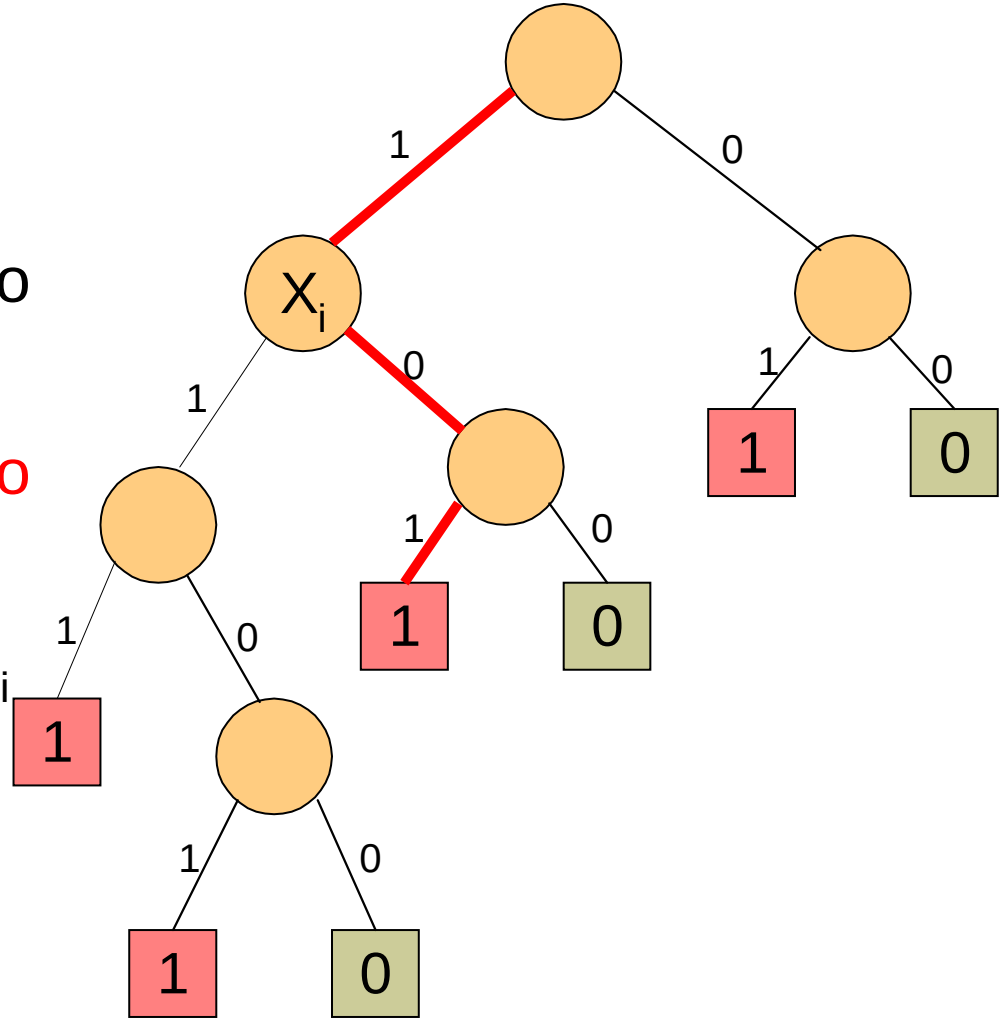


Criticality Function: Routes to a terminal-1

Criticality for X_i

Three Options:

1. paths through X_i on its 1-branch to a terminal-1
2. paths through X_i on its 0-branch to a terminal-1
3. paths which don't pass through X_i on way to a terminal-1

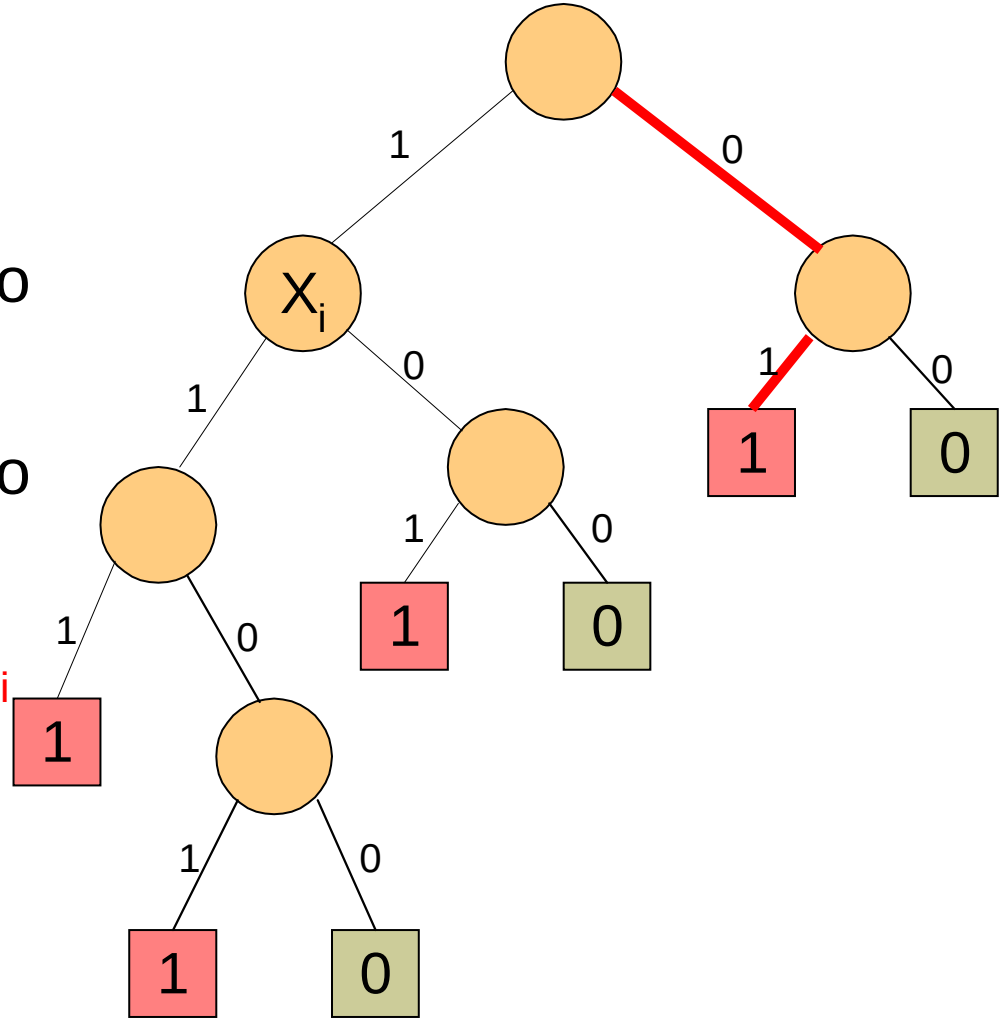


Criticality Function: Routes to a terminal-1

Criticality for X_i

Three Options:

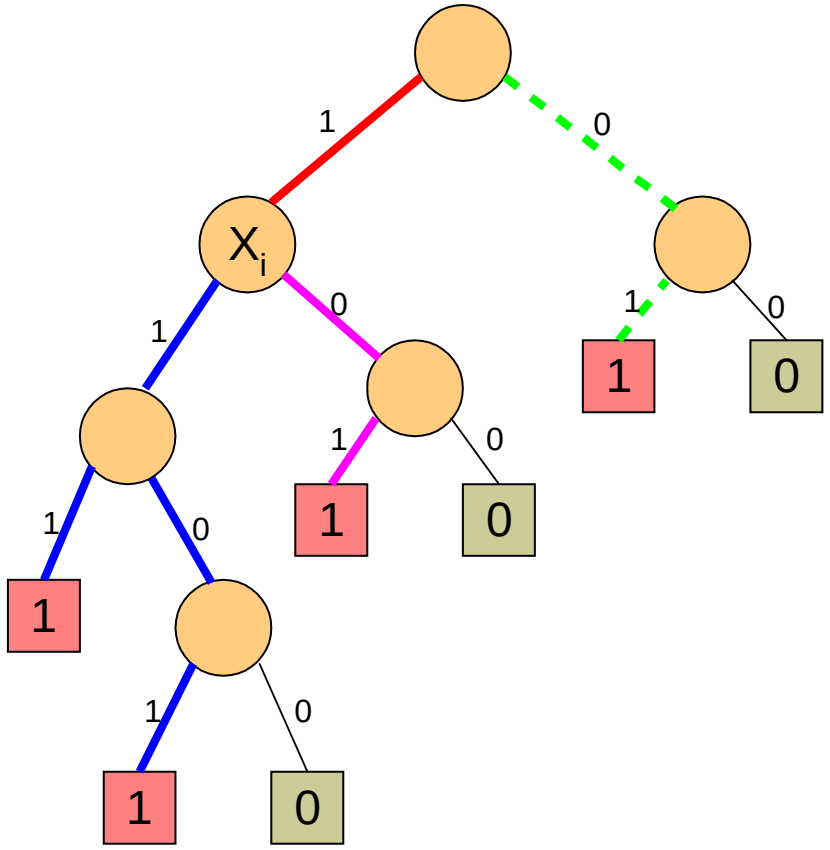
1. paths through X_i on its 1-branch to a terminal-1
2. paths through X_i on its 0-branch to a terminal-1
3. paths which don't pass through X_i on way to a terminal-1



Criticality Function

$$Q(1_i, \underline{q}) = \sum_{i=1}^{n} (pr_{xi}(\underline{q}).po^{1}_{xi}(\underline{q})) + Z(\underline{q})$$

$$Q(0_i, \underline{q}) = \sum_{i=1}^{n} (pr_{xi}(\underline{q}).po^{0}_{xi}(\underline{q})) + Z(\underline{q})$$



$pr_{xi}(\underline{q})$ is the probability of the path section from the root node to node x_i.

$po^{1}_{xi}(\underline{q})$ is the probability of the path section from the 1 branch of node x_i to a terminal 1 node (excluding probability of x_i).

$po^{0}_{xi}(\underline{q})$ is the probability of the path section from the 0 branch of node x_i to a terminal 1 node (excluding probability of x_i).

$Z(\underline{q})$ is the probability of the paths from the root node to the terminal 1 node not passing through the node for variable x_i.

Criticality Function

$$G_i(\boldsymbol{q}) = Q_{SYS}(1_i, \boldsymbol{q}) - Q_{SYS}(1_i, \boldsymbol{q})$$

$$Q_{SYS}(1_i, \boldsymbol{q}) = \sum_{i=1}^{n} (pr_{xi}(\boldsymbol{q}).\, po_{xi}^{1}(\boldsymbol{q})) + Z(\boldsymbol{q})$$

$$Q_{SYS}(0_i, \boldsymbol{q}) = \sum_{i=1}^{n} (pr_{xi}(\boldsymbol{q}).\, po_{xi}^{0}(\boldsymbol{q})) + Z(\boldsymbol{q})$$

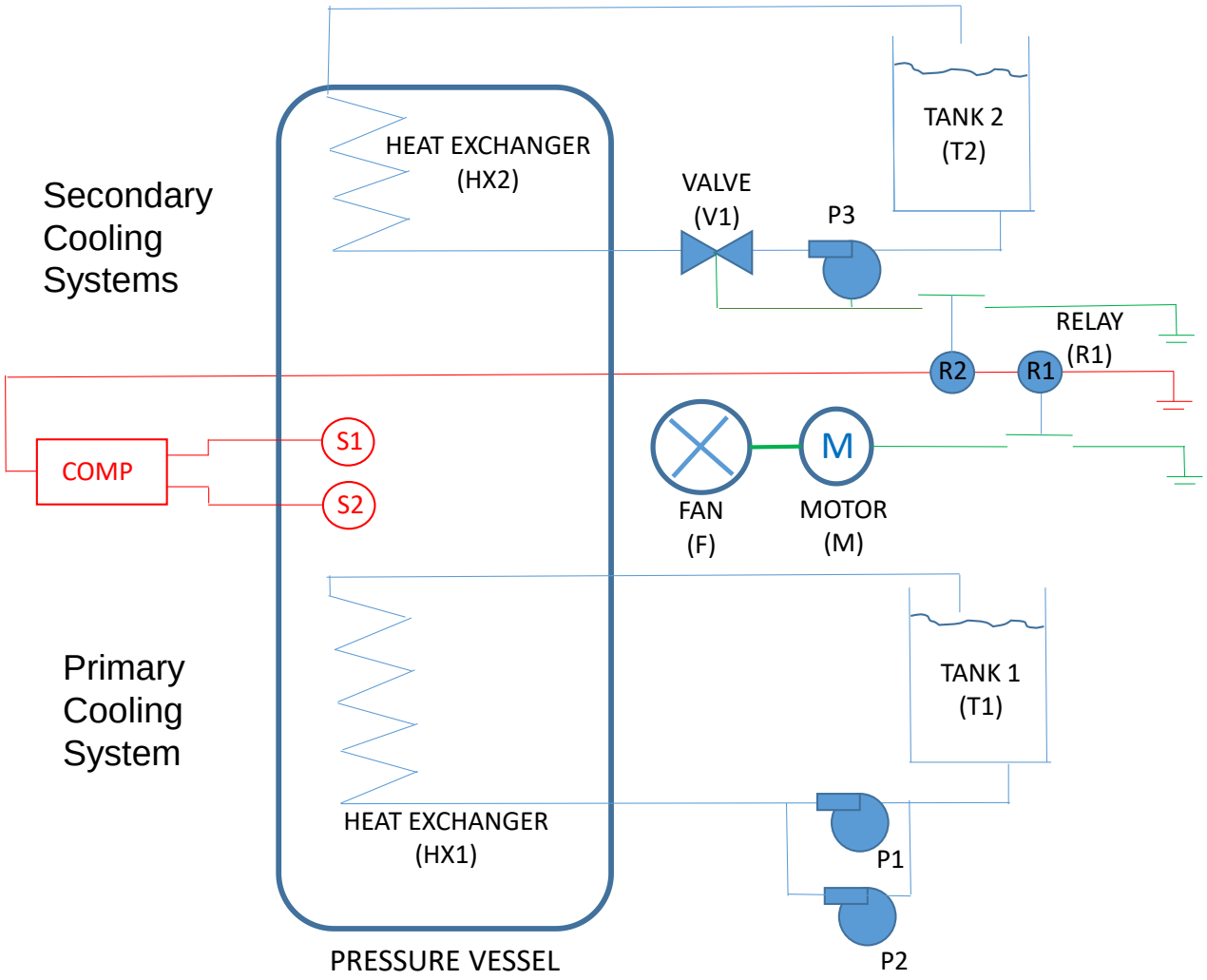
$$G_i(\boldsymbol{q}) = \sum_{i=1}^{n} pr_{xi}(\boldsymbol{q}) \left[po_{xi}^{1}(\boldsymbol{q})) - po_{xi}^{0}(\boldsymbol{q})) \right]$$

$$w_{SYS}(t) = \sum_{\substack{i \\ initiators}} G_i(\boldsymbol{q}).\, w_i\,(t)$$

University of Nottingham
UK | CHINA | MALAYSIA

Case Study

Plant Cooling System and Features

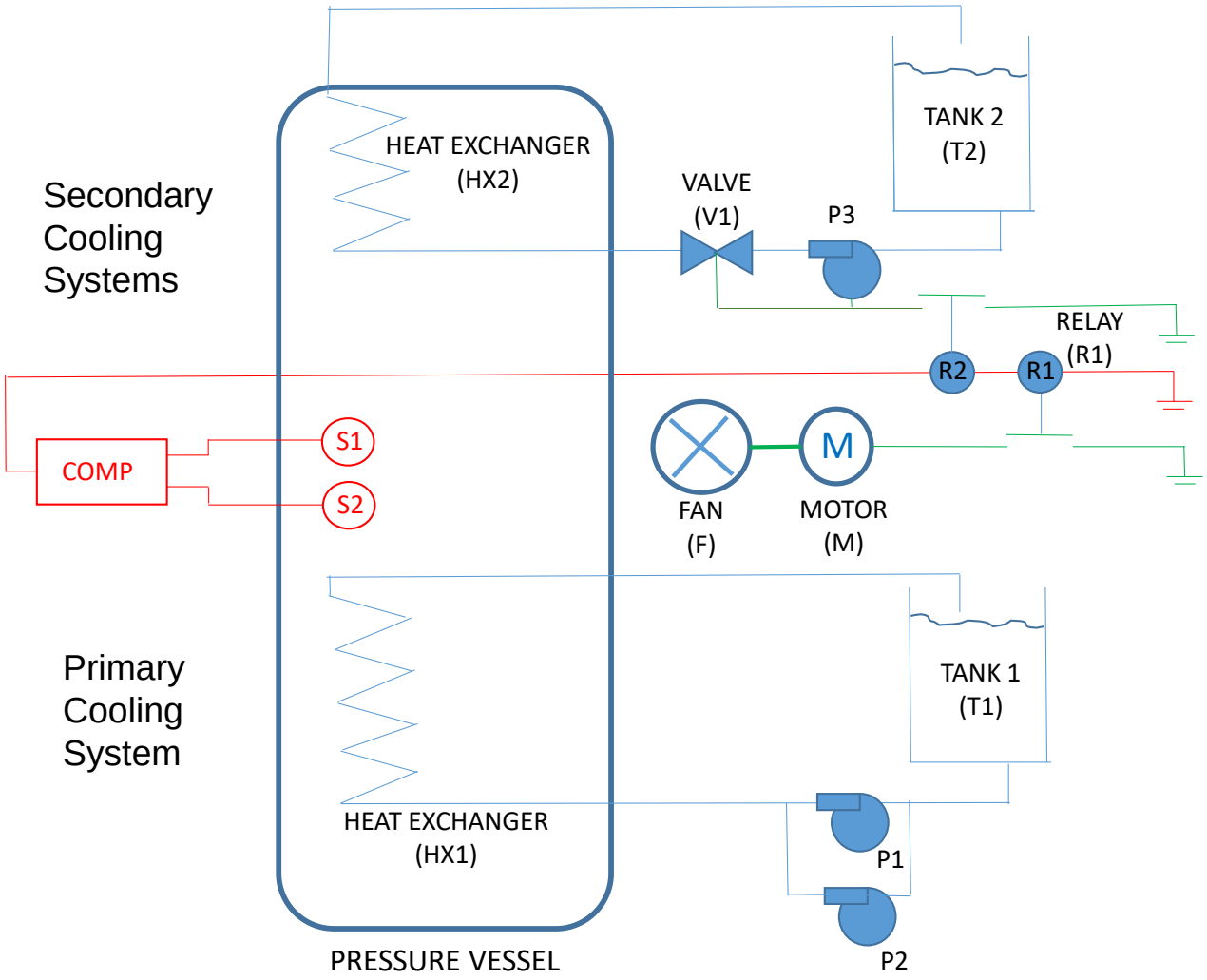


Power supply to all pumps and the valve – B1

Sub-Systems

- Primary Cooling Water System
  - Tank (T1), Pumps (P1,P2), Heat Exchanger (Hx1), Power Supply (B1)
- Detection System
  - Sensors (S1,S2), Computer (Comp)
- Secondary Cooling Water System
  - Tank(T2), Pump (P3), Heat Exchanger (Hx2), Valve (V1), Relay (R2), Power Supply (B1)
- Secondary Cooling Fan System
  - Fan (F), Motor (M), Relay (R1)

Plant Cooling System and Features



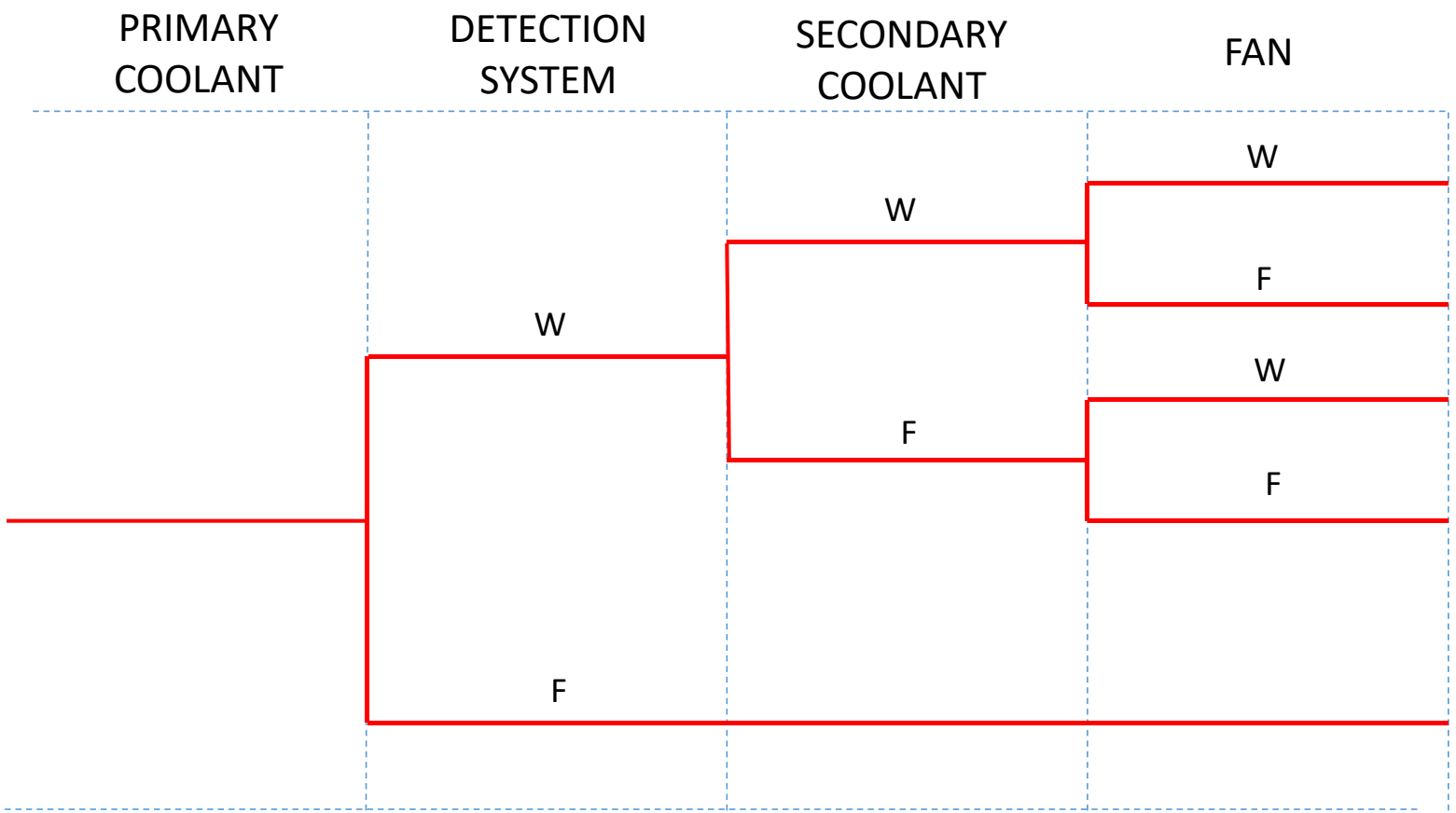
Power supply to all pumps and the valve – B1

Complex Features

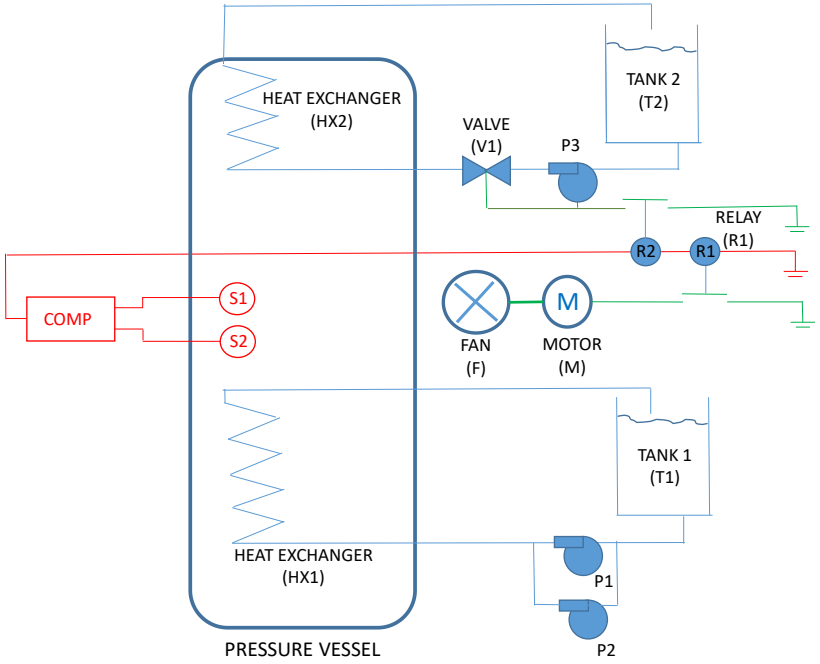
- Non-constant failure / repair rates
  - Relays R1 & R2 have a Weibull failure time distribution and a lognormal repair time distribution
- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other
  - Sensors, S1 and S2 have a common cause calibration failure
  - Tanks T1 and T2, when one fails both are replaced
- Maintenance process
  - The motor, M, has a condition monitoring system with different maintenance actions depending on the condition state.

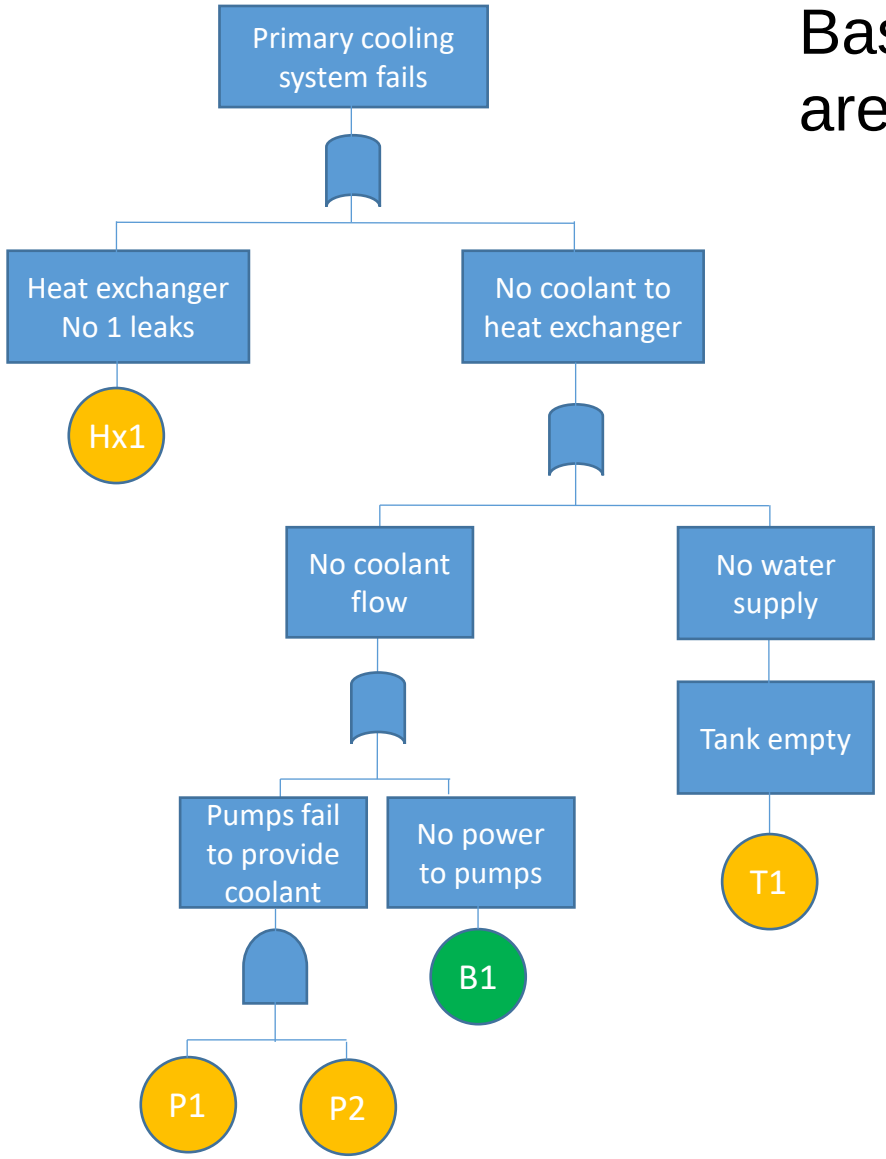
University of Nottingham
UK | CHINA | MALAYSIA

Event Tree Analysis



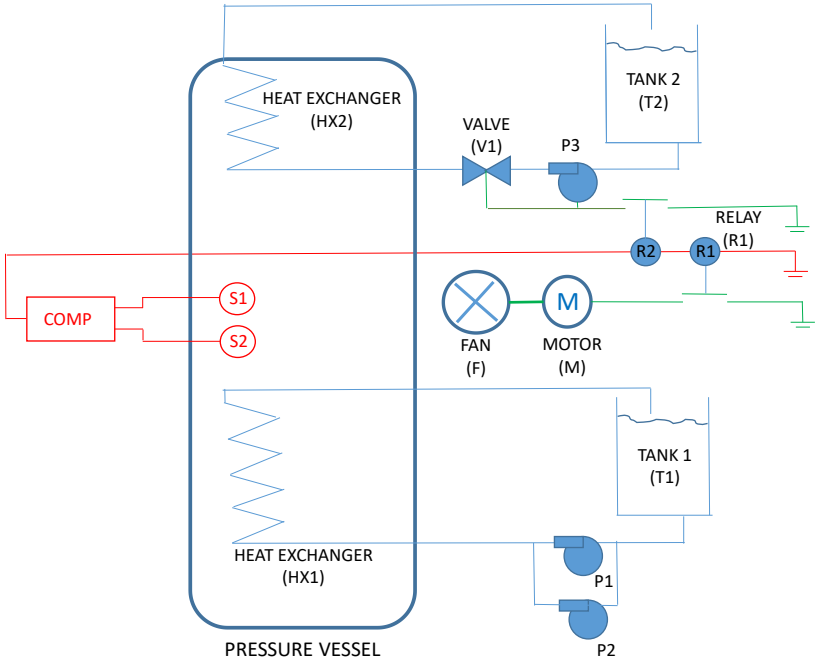
Fault Tree – Primary Cooling Water System



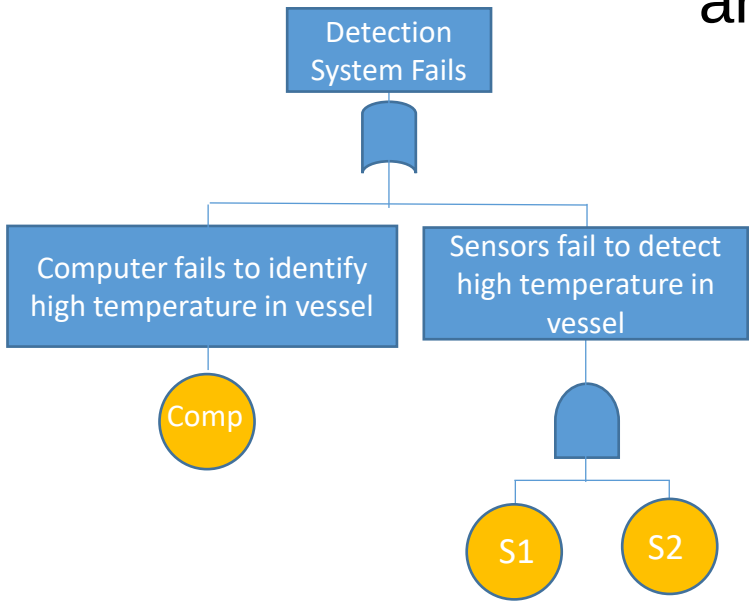


Basic Events are initiators

Fault Tree – Detection System

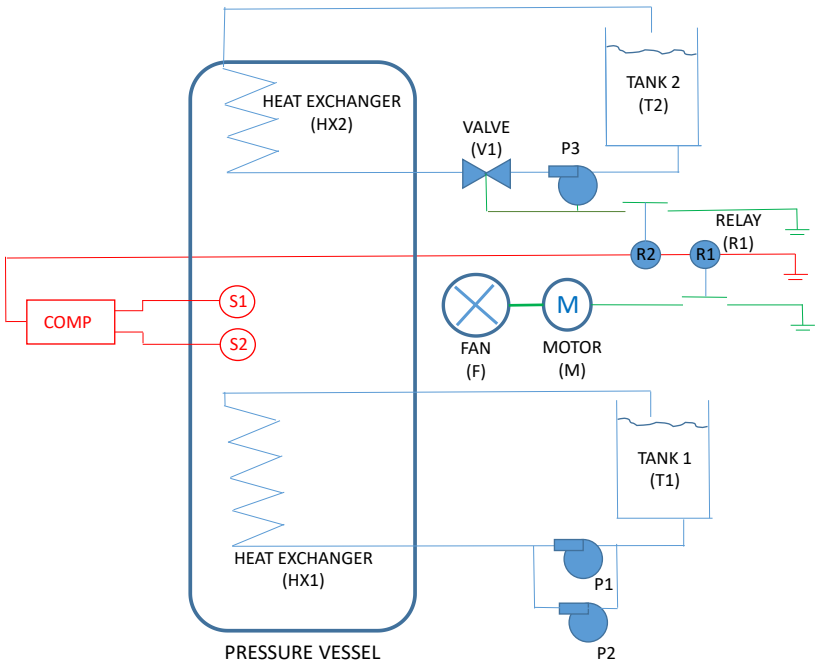


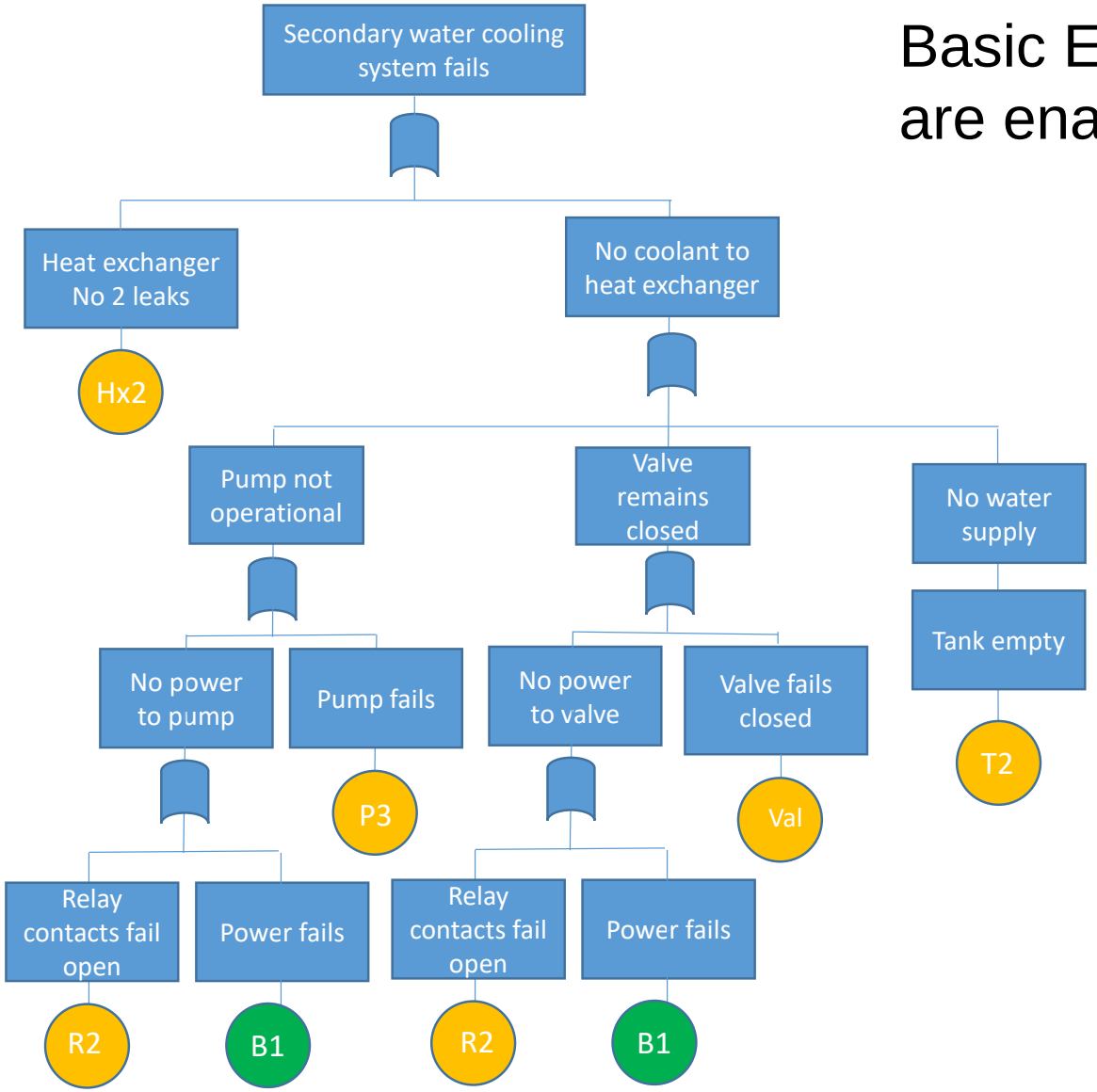
Basic Events are enablers



University of Nottingham
UK | CHINA | MALAYSIA

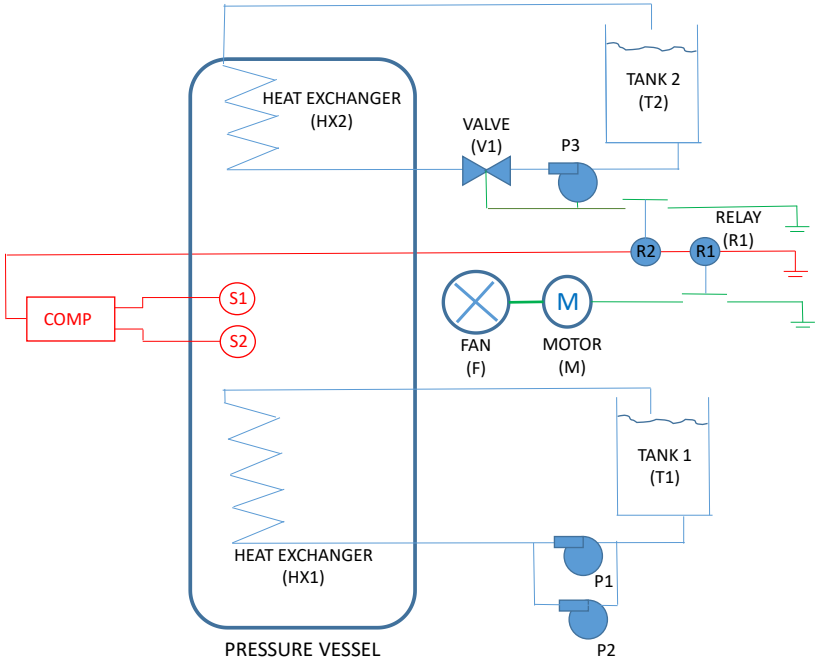
Fault Tree – Secondary Cooling Water System

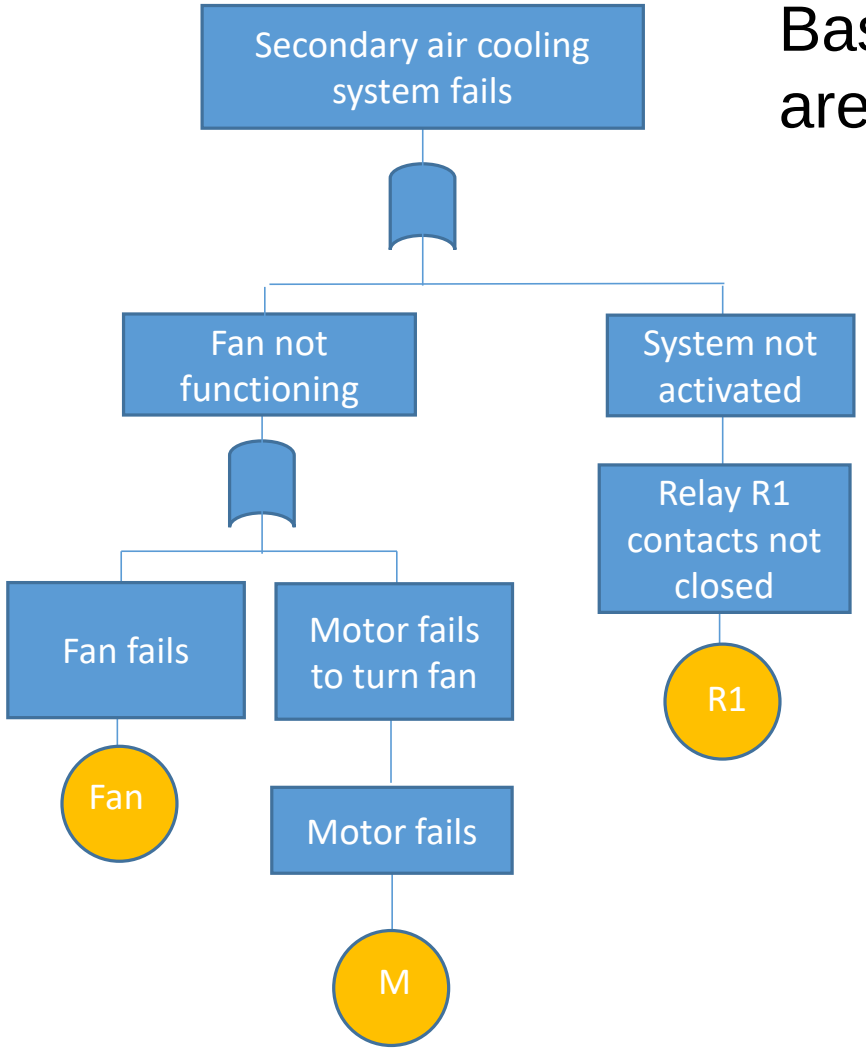




Basic Events are enablers

Fault Tree – Fan Cooling System

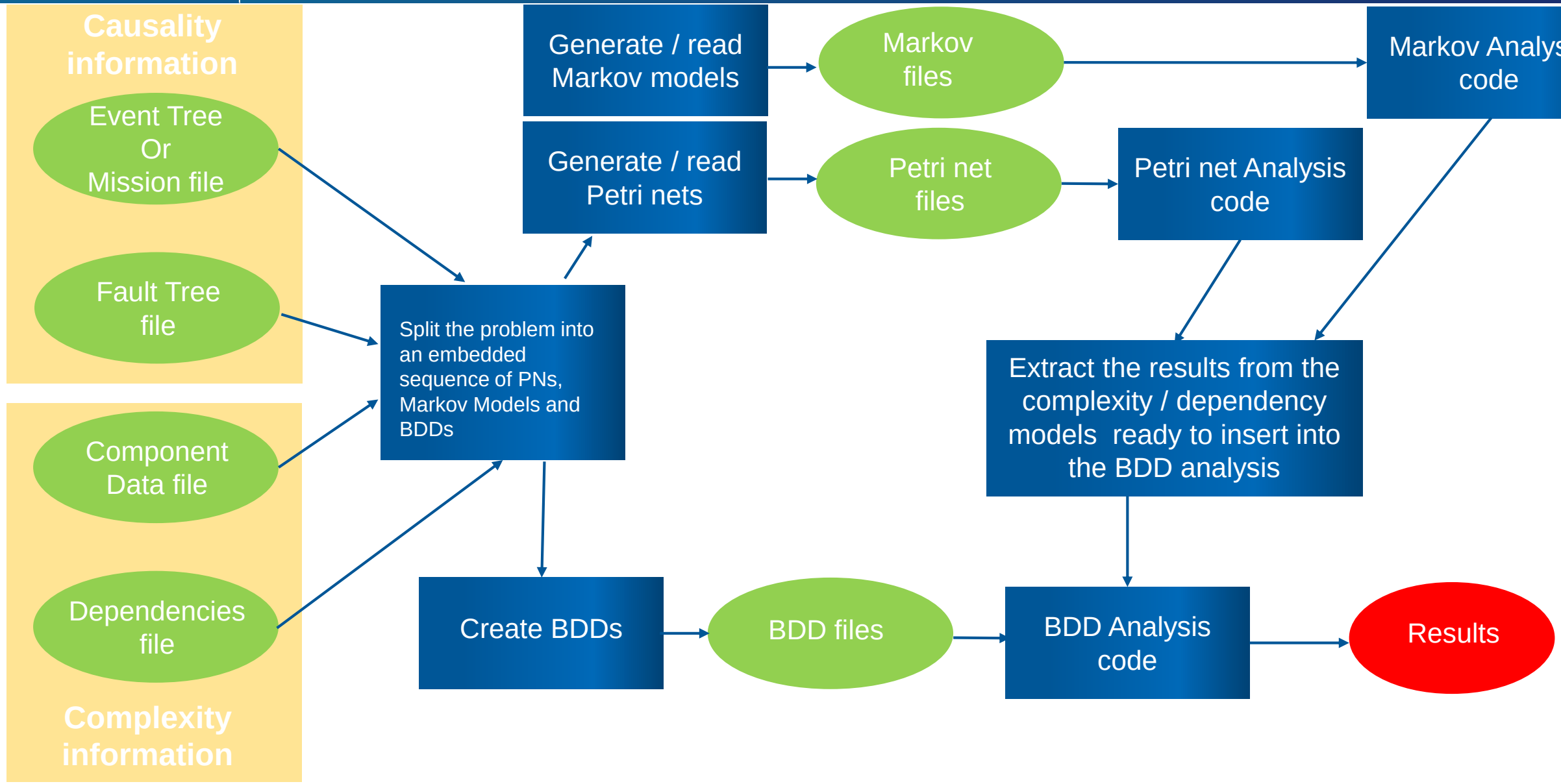




Basic Events are enablers

University of Nottingham
UK | CHINA | MALAYSIA

Basic Structure of the Code



University of Nottingham
UK | CHINA | MALAYSIA

Step 1

Associate the complex features with the fault trees

Identify the complexity / dependency models

Complex Features

- Non-constant failure / repair rates **(DM1)**
  - Relays R1 & R2 have a Weibull failure time distribution and a lognormal repair time distribution

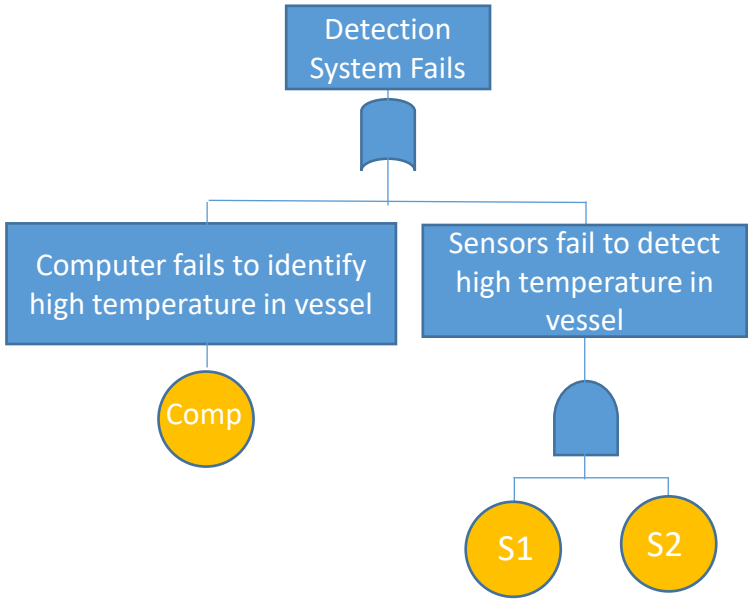
- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other **(DM2)**
  - Sensors, S1 and S2 have a common cause calibration failure **(DM3)**
  - Tanks T1 and T2, when one fails both are replaced **(DM4)**

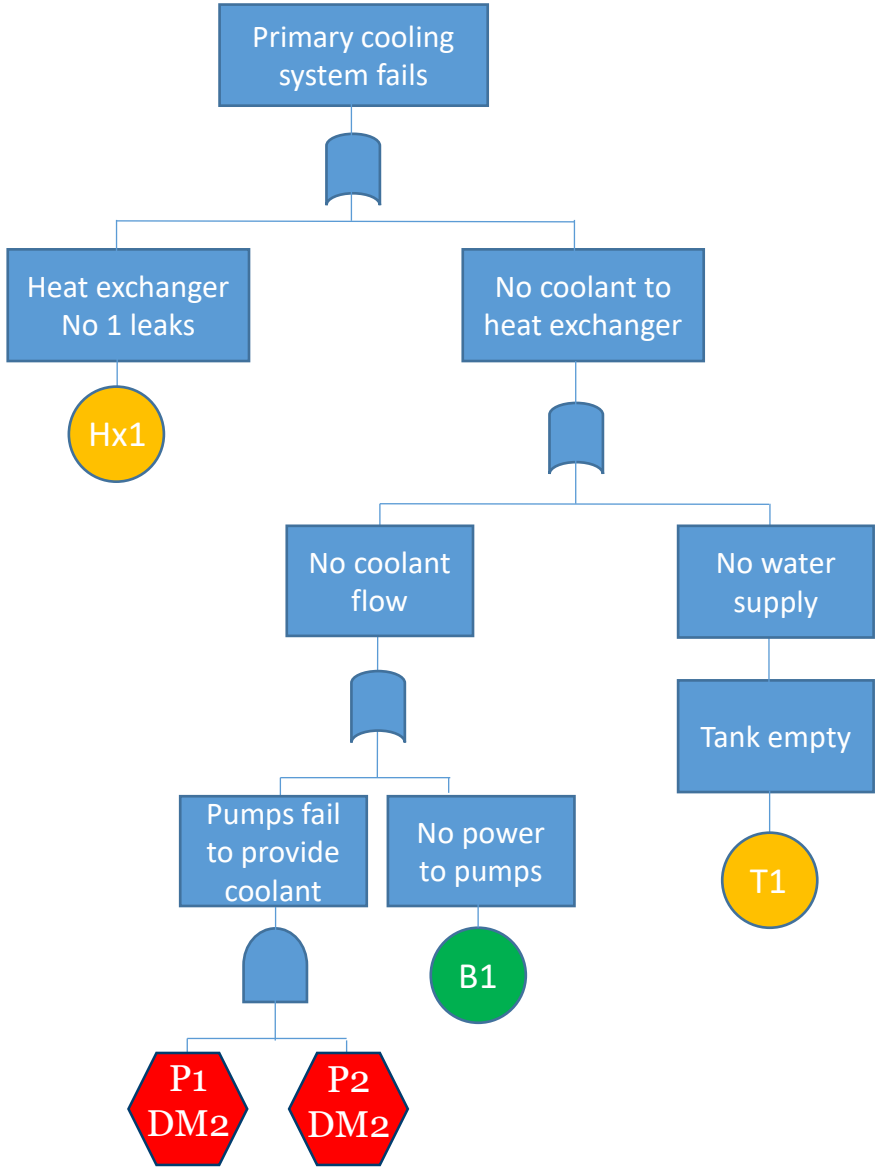
- Maintenance process
  - The motor, M, has a condition monitoring system with different maintenance actions depending on the condition state. **(DM5)**

Fault Tree – Primary Cooling Water System

Complex Features

- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other **(DM2)**

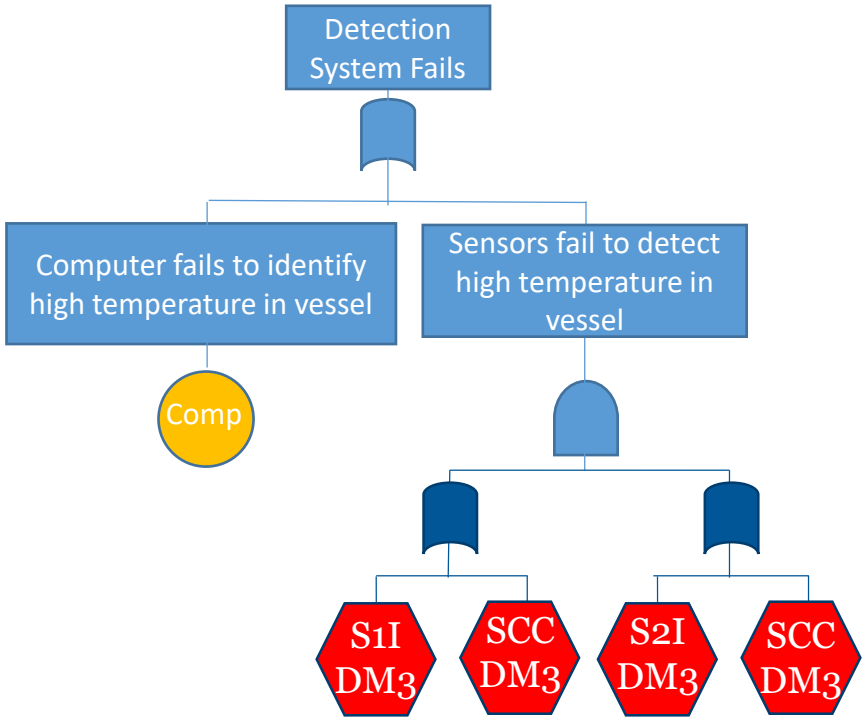


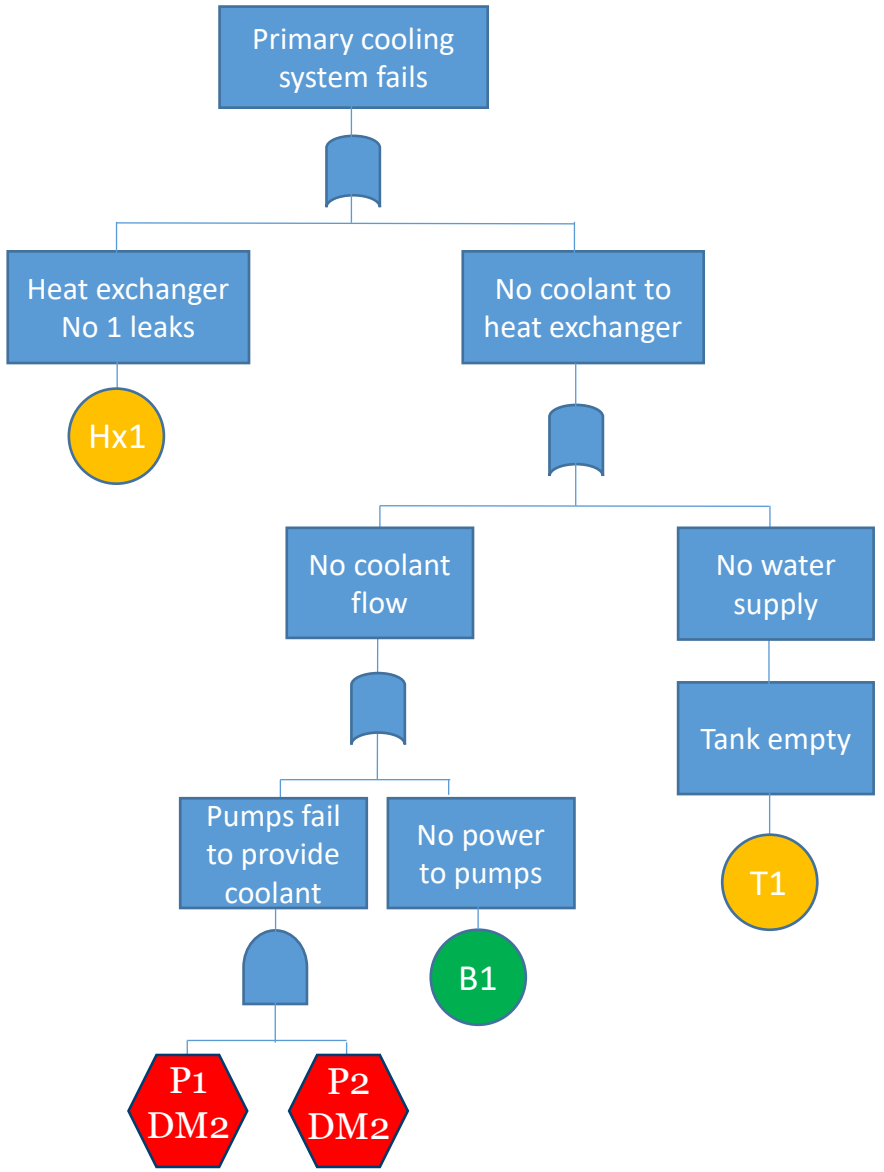


Fault Tree – Primary Cooling Water System

Complex Features

- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other **(DM2)**
  - Sensors, S1 and S2 have a common cause calibration failure **(DM3)**

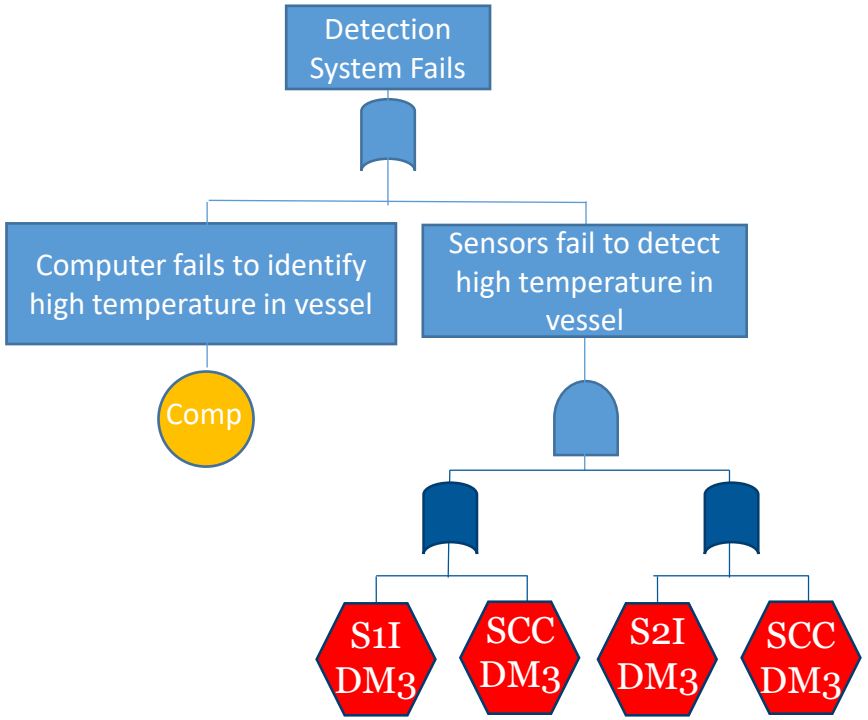


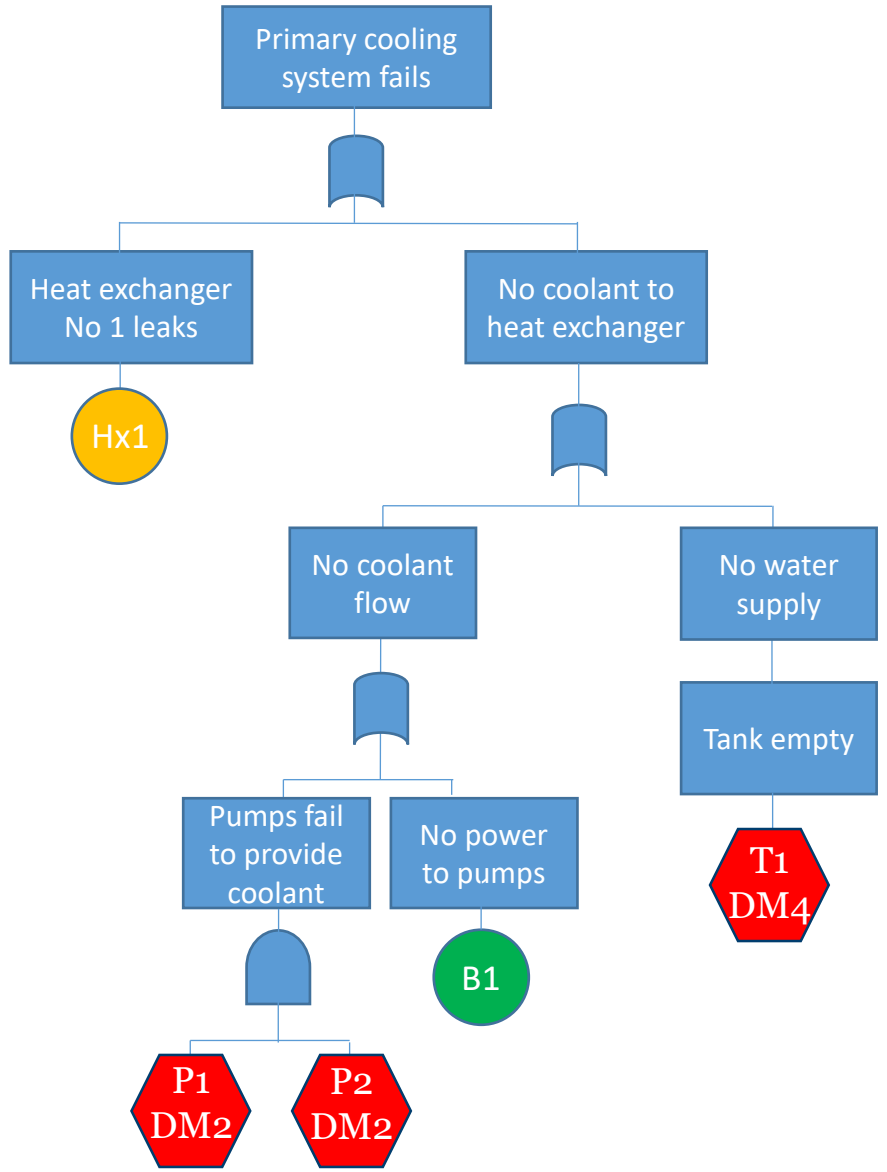


Fault Tree – Primary Cooling Water System

Complex Features

- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other **(DM2)**
  - Sensors, S1 and S2 have a common cause calibration failure **(DM3)**
  - Tanks T1 and T2, when one fails both are replaced **(DM4)**

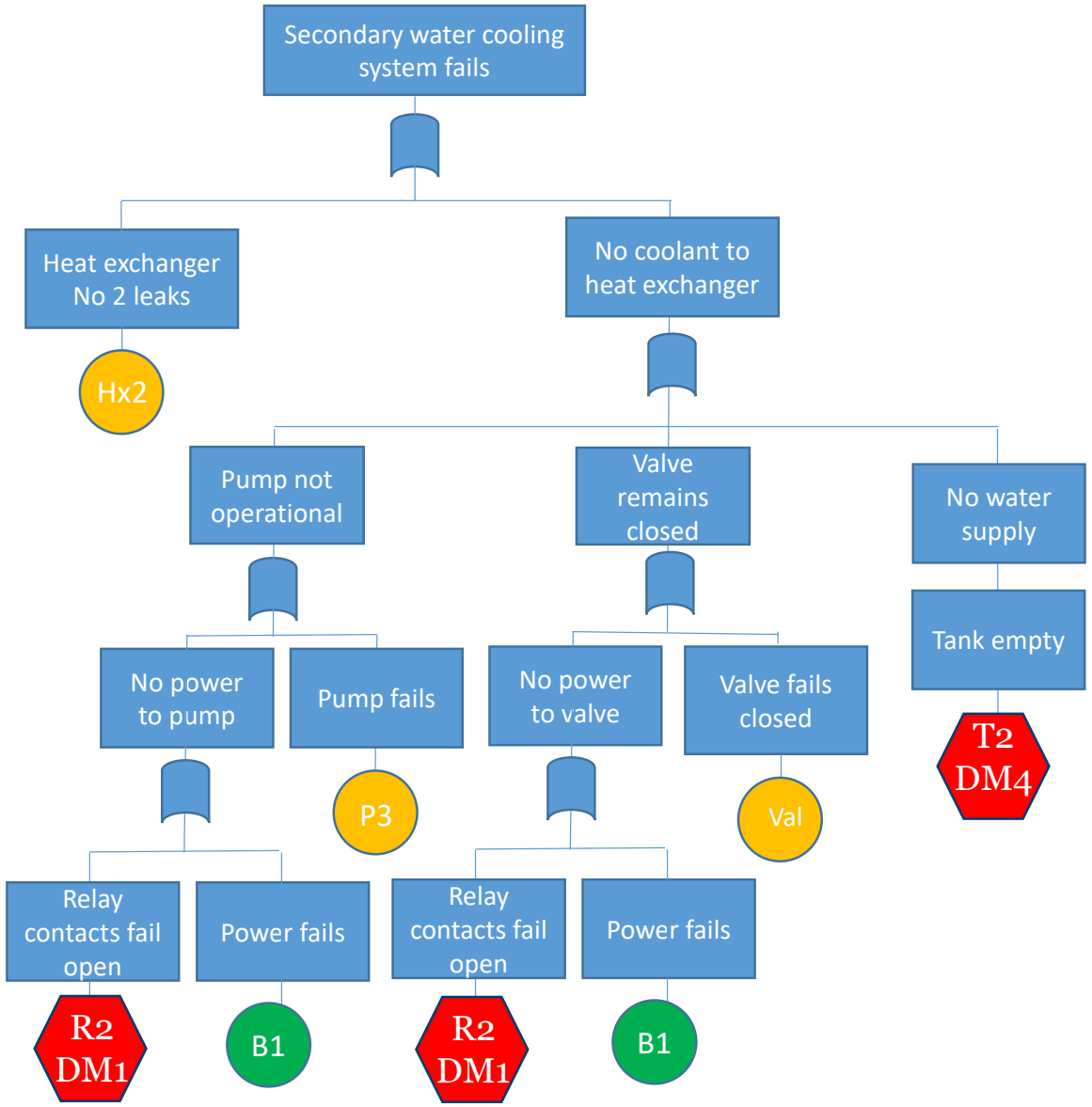




Fault Tree – Secondary Cooling Water System

Complex Features

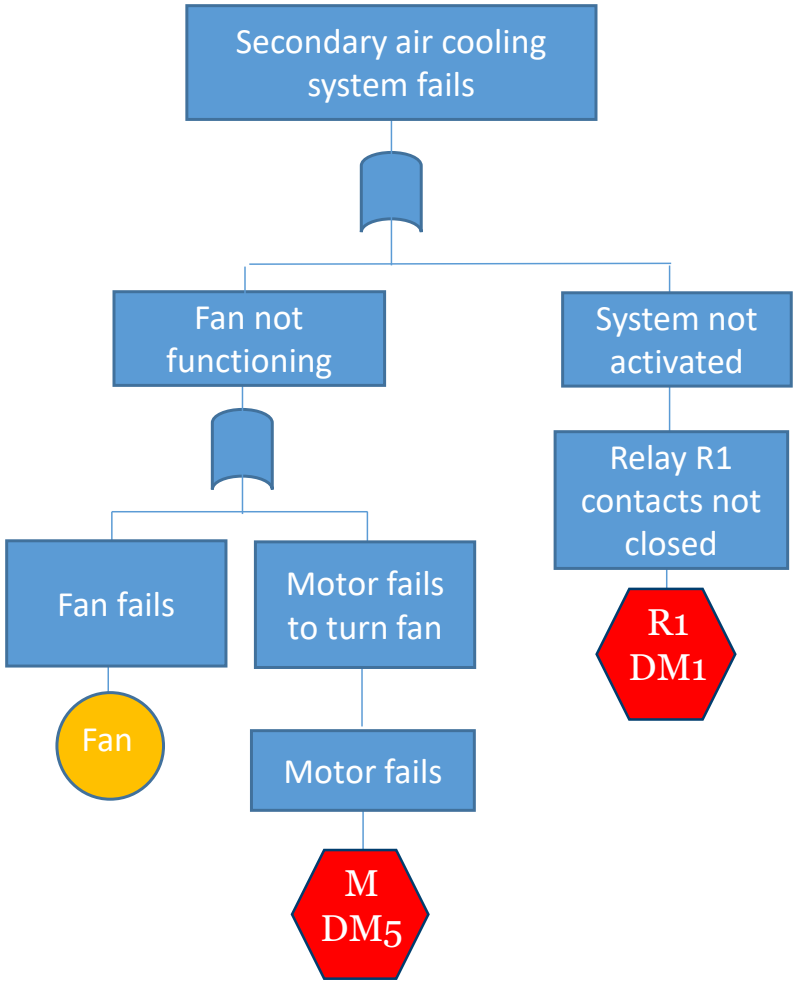
- Non-constant failure / repair rates **(DM1)**
  - Relays R1 & R2 have a Weibull failure time distribution and a lognormal repair time distribution
- Dependencies
  - Tanks T1 and T2, when one fails both are replaced **(DM4)**



Fault Tree – Fan Cooling System

Complex Features

- Non-constant failure / repair rates **(DM1)**
  - Relays R1 & R2 have a Weibull failure time distribution and a lognormal repair time distribution
- Maintenance process
  - The motor, M, has a condition monitoring system with different maintenance actions depending on the condition state. **(DM5)**




University of
Nottingham
UK | CHINA | MALAYSIA
Step 2
Calculate simple component failure models

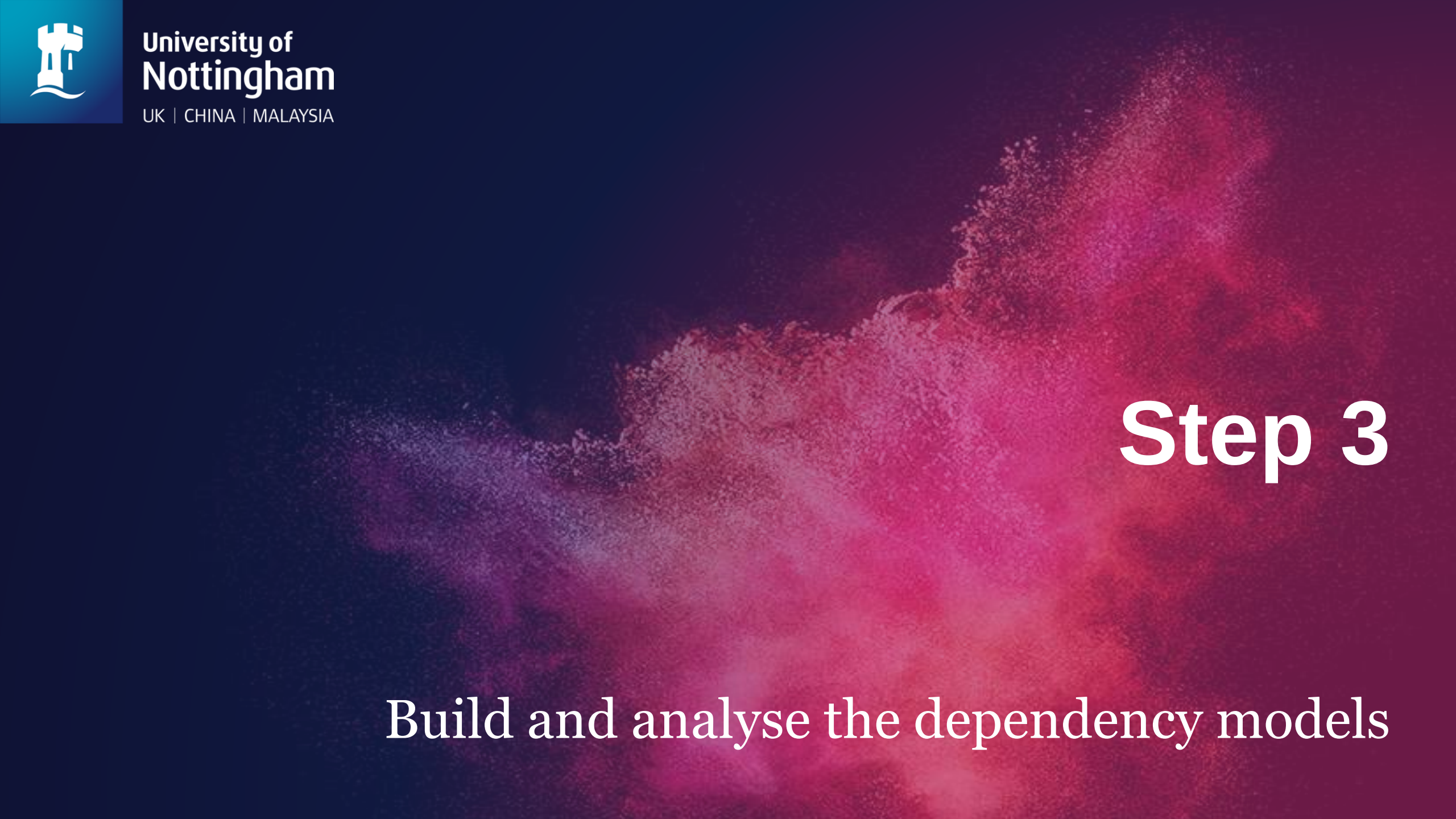
Simple Component Failure Models

Revealed Failures - initiators

Component	Code	Failure rate (λ) Per year	Mean time to repair (τ) years	Failure Probability $q=\frac{\lambda}{\lambda+\nu}$	Failure Intensity w=λ(1-q)
Heat Exchanger	HX1	0.125	5.5×10^{-3}	6.8703×10^{-4}	0.1249
Power Supply	B1	0.5	2.5×10^{-3}	1.248×10^{-3}	0.4994

Unrevealed Failures - enablers

Component	Code	Failure rate (λ) Per year	Mean time to repair (τ) years	Inspection int (θ) years	q=λ(θ/2+τ)
Heat Exchanger	HX2	0.125	5.5×10^{-3}	1	0.06319
Computer	Comp	0.4	5.0×10^{-3}	0.08	0.034
Pump	P3	0.05	0.08333	0.5	0.01667
Fan	Fan	0.06	5.0×10^{-3}	0.5	0.0153


University of
Nottingham
UK | CHINA | MALAYSIA
Step 3
Build and analyse the dependency models

Identify the complexity / dependency models

Complex Features

- Non-constant failure / repair rates **(DM1)**
  - Relays R1 & R2 have a Weibull failure time distribution and a lognormal repair time distribution

- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other **(DM2)**
  - Sensors, S1 and S2 have a common cause calibration failure **(DM3)**
  - Tanks T1 and T2, when one fails both are replaced **(DM4)**

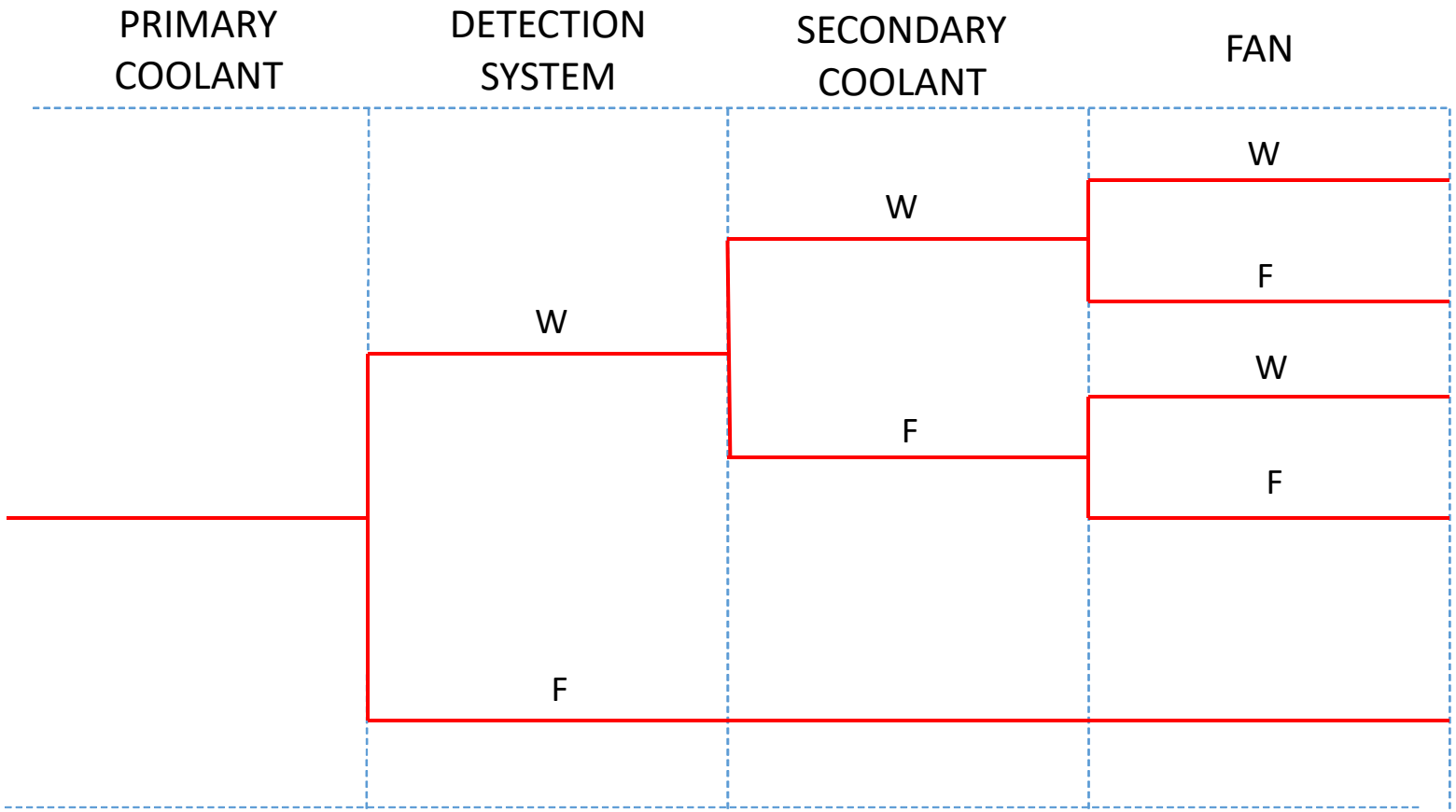
- Maintenance process
  - The motor, M, has a condition monitoring system with different maintenance actions depending on the condition state. **(DM5)**

University of Nottingham
UK | CHINA | MALAYSIA

Step 4

Consider the causes of each Event Tree outcome

Event Tree Analysis



5 $P(DET_w)P(FAN_w)w(SEC_w.PC_f)$

4 $P(DET_w)P(FAN_f)w(SEC_w.PC_f)$

3 $P(DET_w)P(FAN_w)w(SEC_f.PC_f)$

2 $P(DET_w)P(FAN_f)w(SEC_f.PC_f)$

1 $P(DET_f).w(PC_f)$

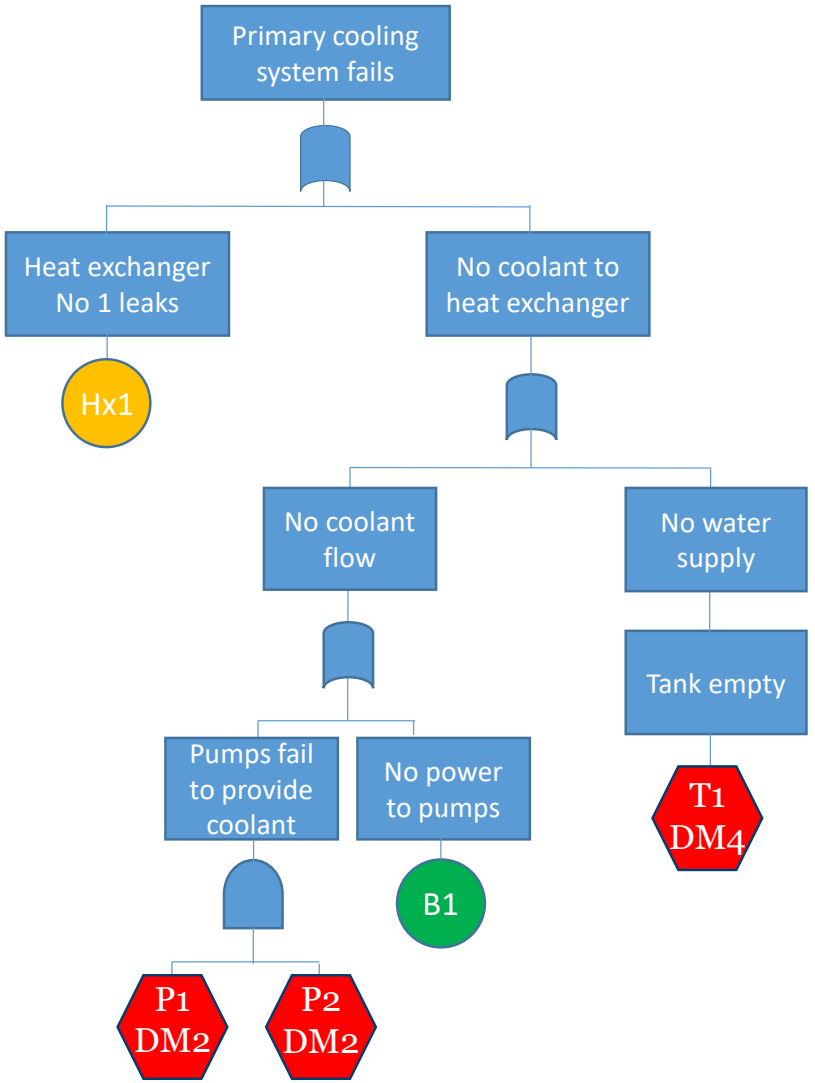
University of Nottingham
UK | CHINA | MALAYSIA

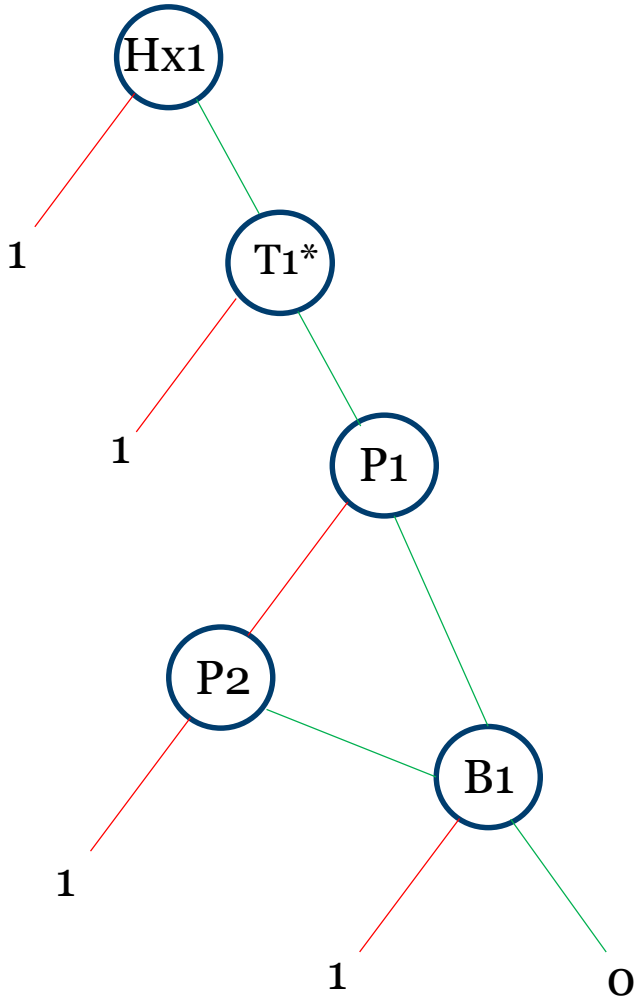
Step 4a Event Tree Outcome -1

Primary Coolant Failure intensity
Detection System fails

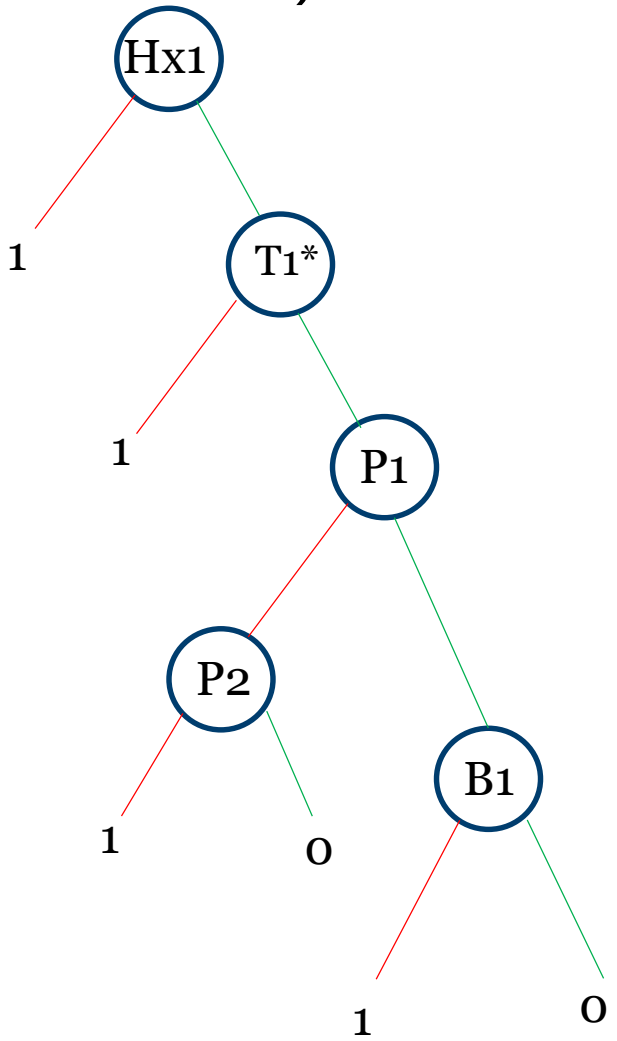
Outcome 1 Primary Coolant failure intensity

Freq1=P(Detection System Fails).w(Primary coolant fails)





BDD

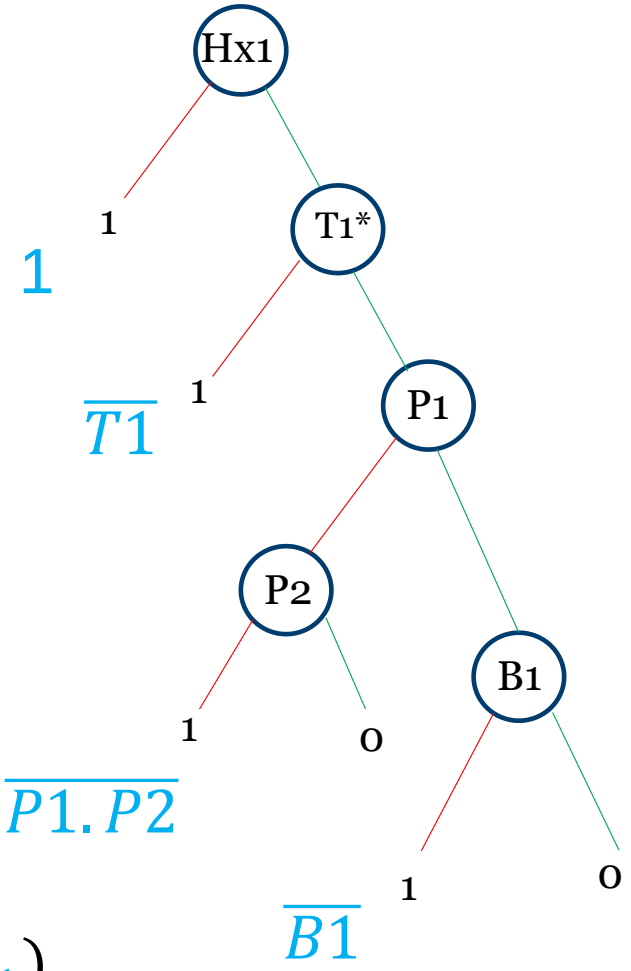


Minimal BDD encoding
Min cut sets

Outcome 1 failure intensity term for Hx1

$$w_{SYS}(t)dt = \sum_{\substack{i \\ initiators}} G_i\big(\boldsymbol{q}(t)\big).w_i\,(t)dt$$

- For a system to be in a critical state for component i the following conditions must exist:
  - The system is not already failed (no min cut sets not containing i can exist)
  - All other events in min cut sets containing event i must have already occurred



P(the system is in a critical state for initiator Hx1 and Hx1 then occurs in [t,t+dt))

$$G_{Hx1}\big(\boldsymbol{q}(t)\big).w_{Hx1}(t)dt = P(\overline{T1}.\overline{P1.P2}.\overline{B1}.w_{Hx1})$$

$$= P(\overline{T1}).P(\overline{B1}).P(\overline{P1.P2})\,P(w_{Hx1})$$

$$= (1-q_{T1}).(1-q_{B1}).(1-q_{P1.P2}).w_{Hx1}dt$$

Outcome 1 failure intensity for Hx1

P(the system is in a critical state for initiator i and i then occurs in [t,t+dt))

$$G_{Hx1}(\boldsymbol{q}(t)).w_{Hx1}(t)dt = (1-q_{T1}).(1-q_{B1}).(1-q_{P1.P2}).w_{Hx1}dt$$

Code	Failure Probability $q=\frac{\lambda}{\lambda+\nu}$	Failure Intensity w=λ(1-q)
HX1	6.8703×10^{-4}	0.1249
B1	1.248×10^{-3}	0.4994

From DM4
P(T1) = 0.008053

From DM2
P(P1.P2) = 0.011764786

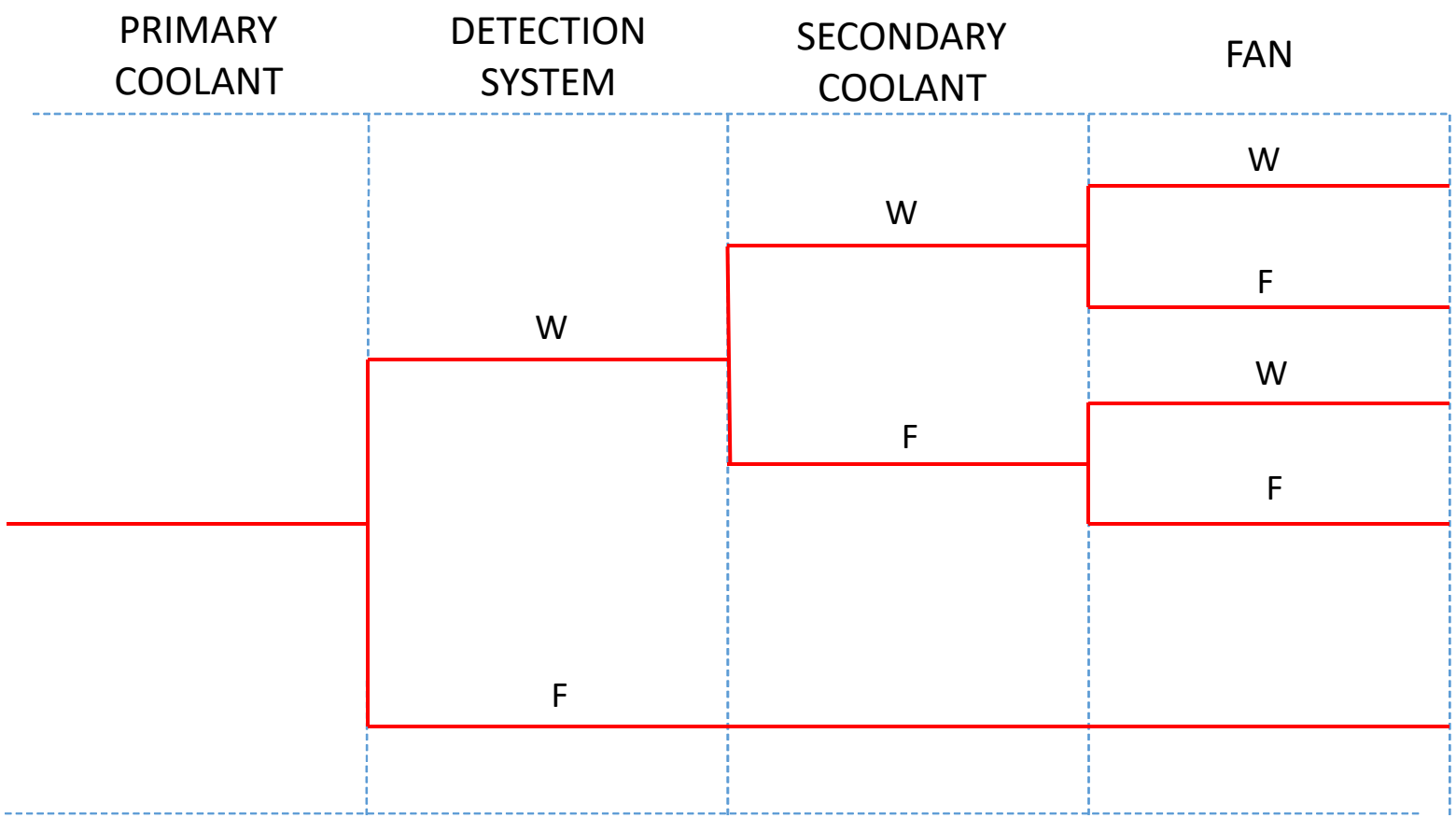
Outcome 1 intensity of initiating event

Similar Calculation for other initiators P1, P2, T1, B1

$$w_{SYS}(t) = \sum_{\substack{i \\ initiators}} G_i\big(\boldsymbol{q}(t)\big).w_i\,(t)$$

Failure Intensity of the Primary Cooling System = 0.780261 per year

Repeating this process for all other events



5 $P(DET_w)P(FAN_w)w(SEC_w.PC_f)$

4 $P(DET_w)P(FAN_f)w(SEC_w.PC_f)$

3 $P(DET_w)P(FAN_w)w(SEC_f.PC_f)$

2 $P(DET_w)P(FAN_f)w(SEC_f.PC_f)$

1 $P(DET_f).w(PC_f)$

$P(DET_f) = 0.132513$

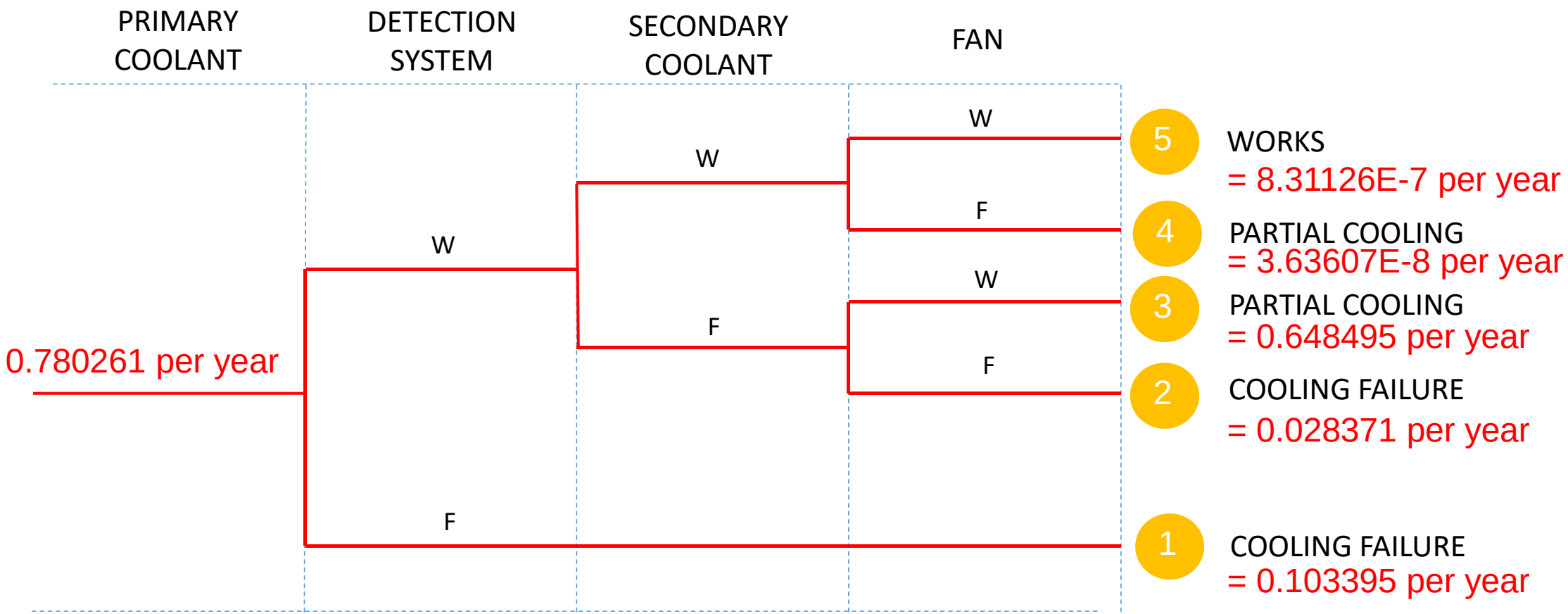
$w(PC_f) = 0.780261$ per year

$P(FAN_f) = 0.041915$

$w(SEC_f.PC_f) = 0.780260$

$w(SEC_w.PC_f) = 1.0e-6$

Event Tree Analysis



Summary / Conclusions

- First Phase of the Next Generation Risk Assessment Methodologies has been described
- This incorporates the following features into the modelling
  - Dependencies
  - Non-constant failure and repair rates
  - Complex maintenance strategies
  - A method has been developed which enables results from the PN/Markov models to be integrated into the BDDs
- Current work:
  - Modularisation methods
  - Building dependencies into the phased mission methodology
  - Solving case studies provide by the aero and railway industries

Thank you for your attention

Any Questions?