University of Nottingham
UK | CHINA | MALAYSIA

Improved Methods for System Reliability Modelling

Professor John Andrews

SPAA & Dependability@Siemens 2023
Nuremberg 8-9 November 2023

University of Nottingham
UK | CHINA | MALAYSIA

Resilience Engineering Research Group

Academic Staff

- Prof John Andrews
- Dr Rasa Remenyte-Prescott
- Dr Luis Neves
- Dr Darren Prescott
- Dr Silvia Tolo
- Dr Derek Yan

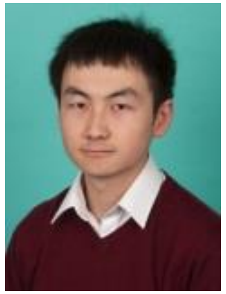
NxGen Project Manager

- Kate Sanderson

Started in 2009 with my appointment to a research chair in Infrastructure Asset Management supported by Network Rail and the Royal Academy of Engineering.

Network Rail

The Royal Academy of Engineering



Research Activities

Modelling to support the prevention of system failures and the mitigation of their consequences

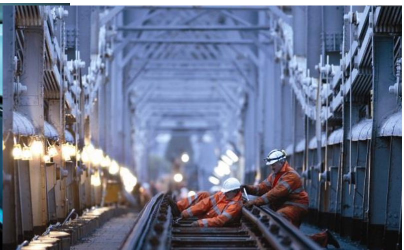
- Risk and Reliability Engineering
- Asset Management
- Resilience Engineering

Industrial Sectors

- Railways
- Nuclear
- Fuel Cell
- Oil & Gas
- Aerospace
- Military
- Manufacturing
- Healthcare



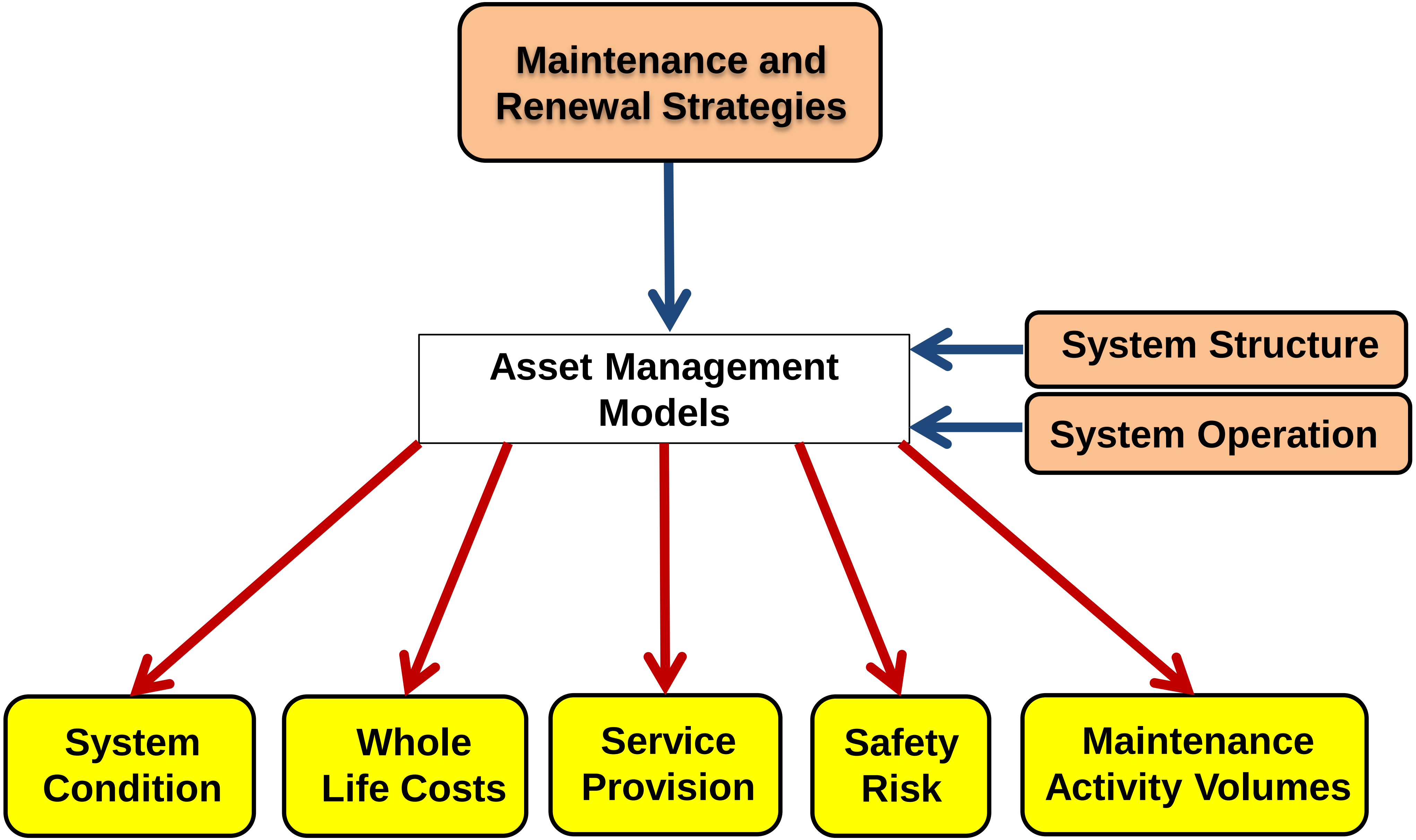


University of Nottingham
UK | CHINA | MALAYSIA

Railway Infrastructure Asset Management

Asset Management Modelling Framework

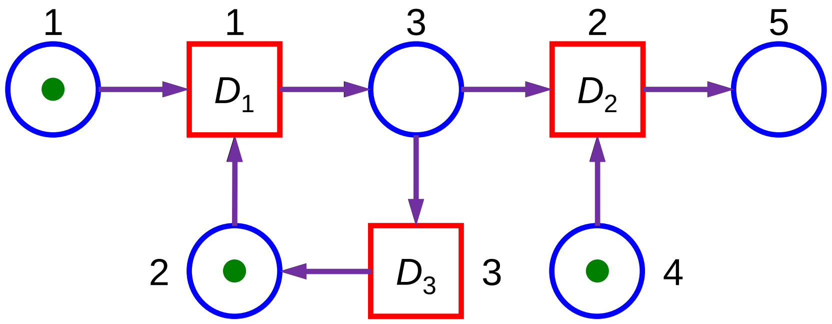


University of Nottingham
UK | CHINA | MALAYSIA

Modelling Method

Petri Nets

Petri Net Basics and Definitions



i

Places, p_i

- Marked with tokens

Edges

- From place to transition or transition to place.

j

D_j

Transitions, t_j

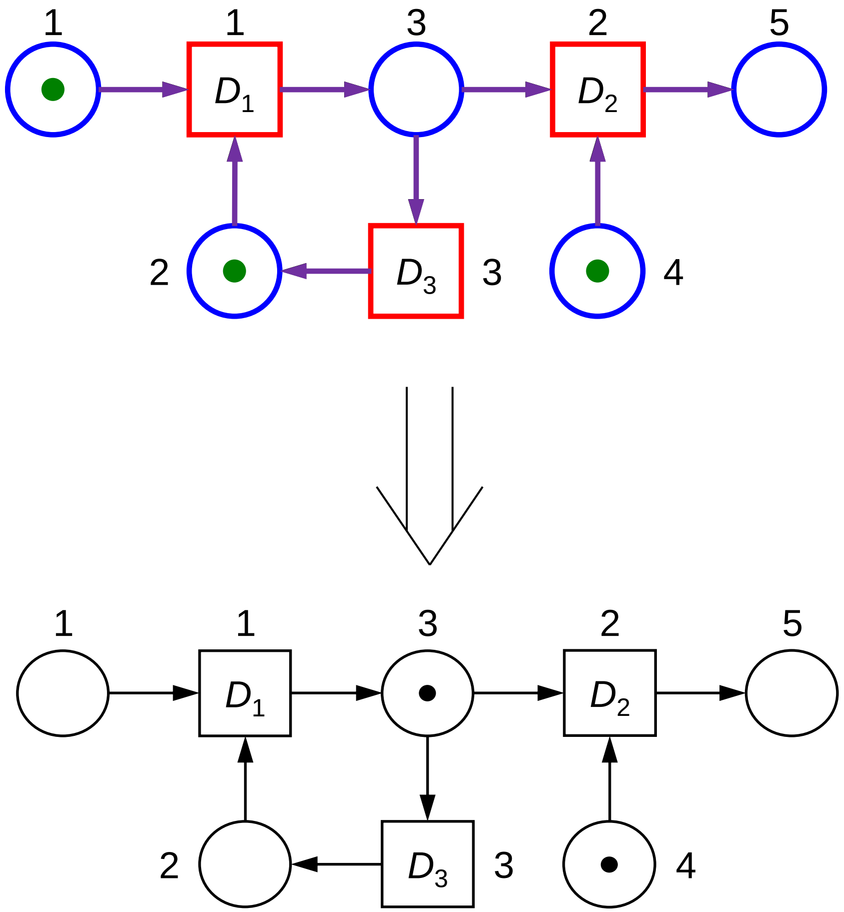
- Time delay D_j determines token movement.
- Type:
  - immediate if $D_j = 0$
  - timed if $D_j \neq 0$

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

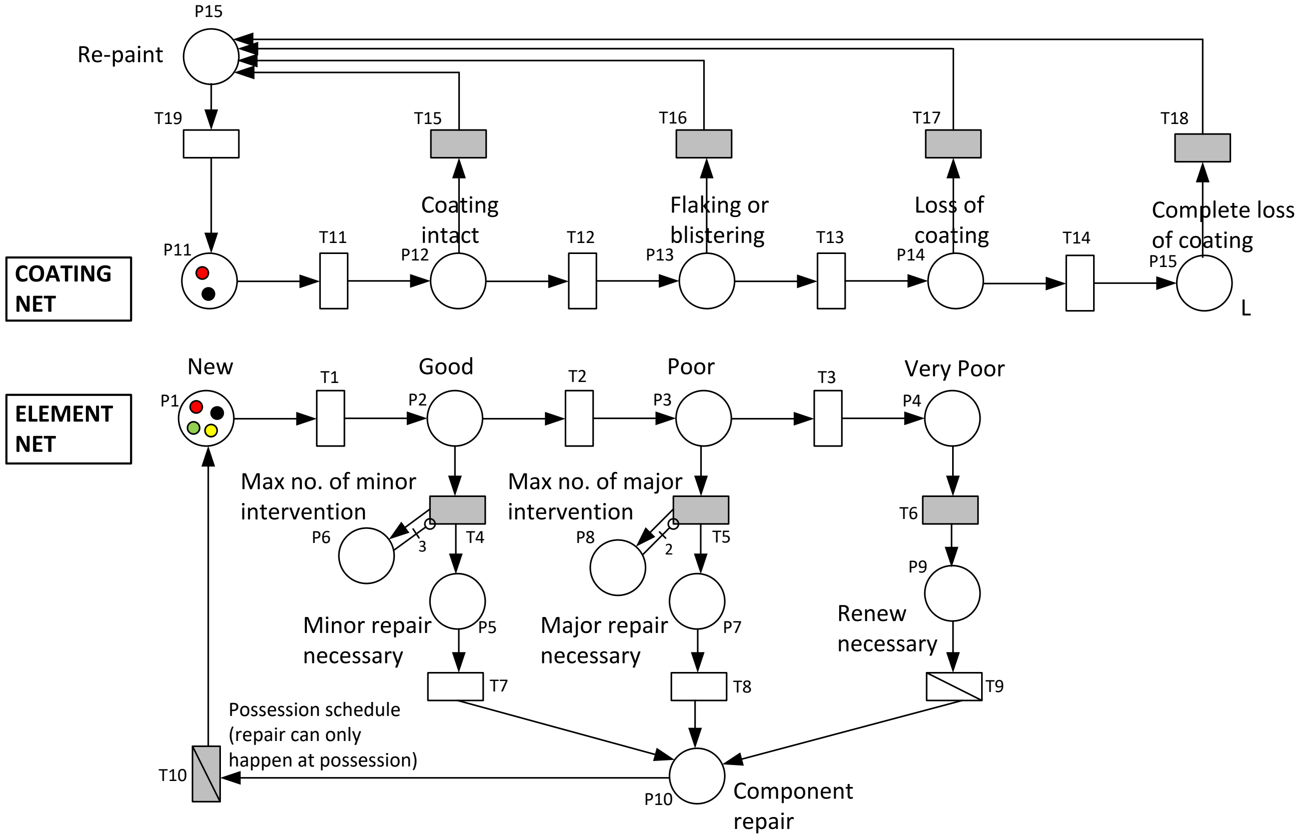
Petri Net Modelling

- 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.



Petri Net Model Features



Features

- Any distribution of times to transition
- Capable of modelling very complex maintenance strategies
- Concise structure
- Solution by Monte Carlo simulation
- Produces distributions of durations and no of incidences of different states
- Easy to modularise and link module models to form system model

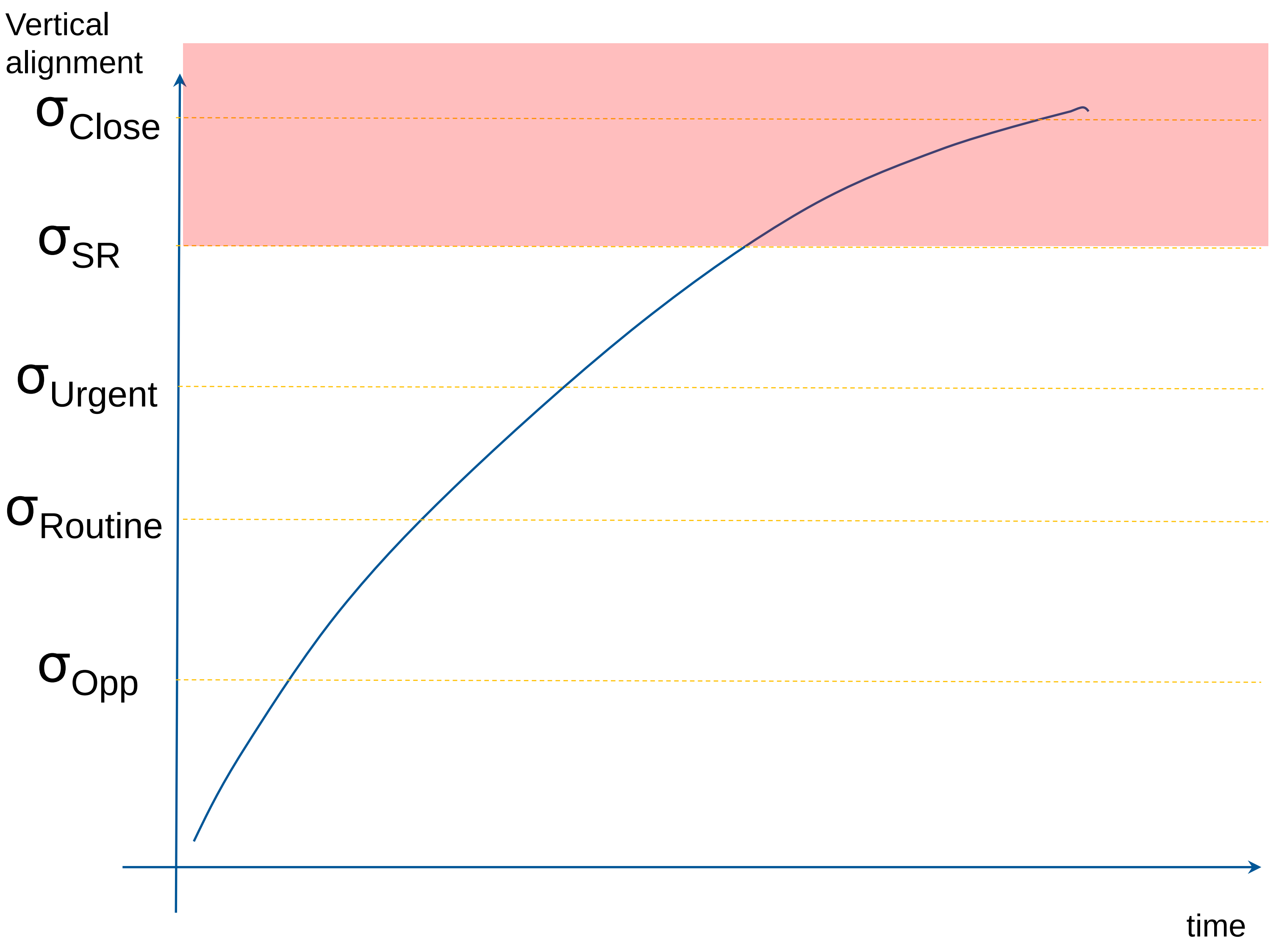
University of Nottingham
UK | CHINA | MALAYSIA

Case Study

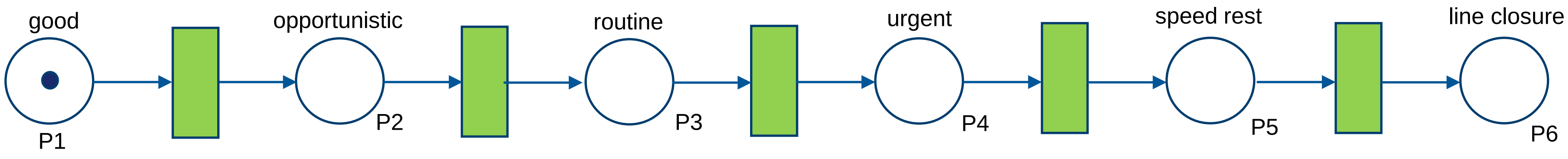
Maintaining Railway Track Geometry

Vertical alignment of 200m sections

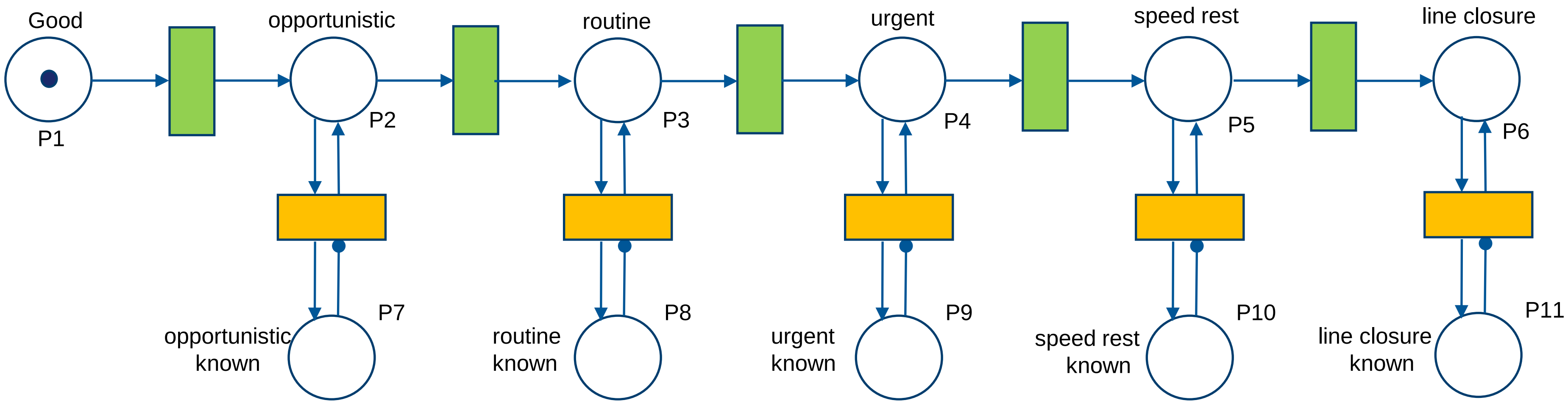
Vertical Alignment Degradation (200 m section)



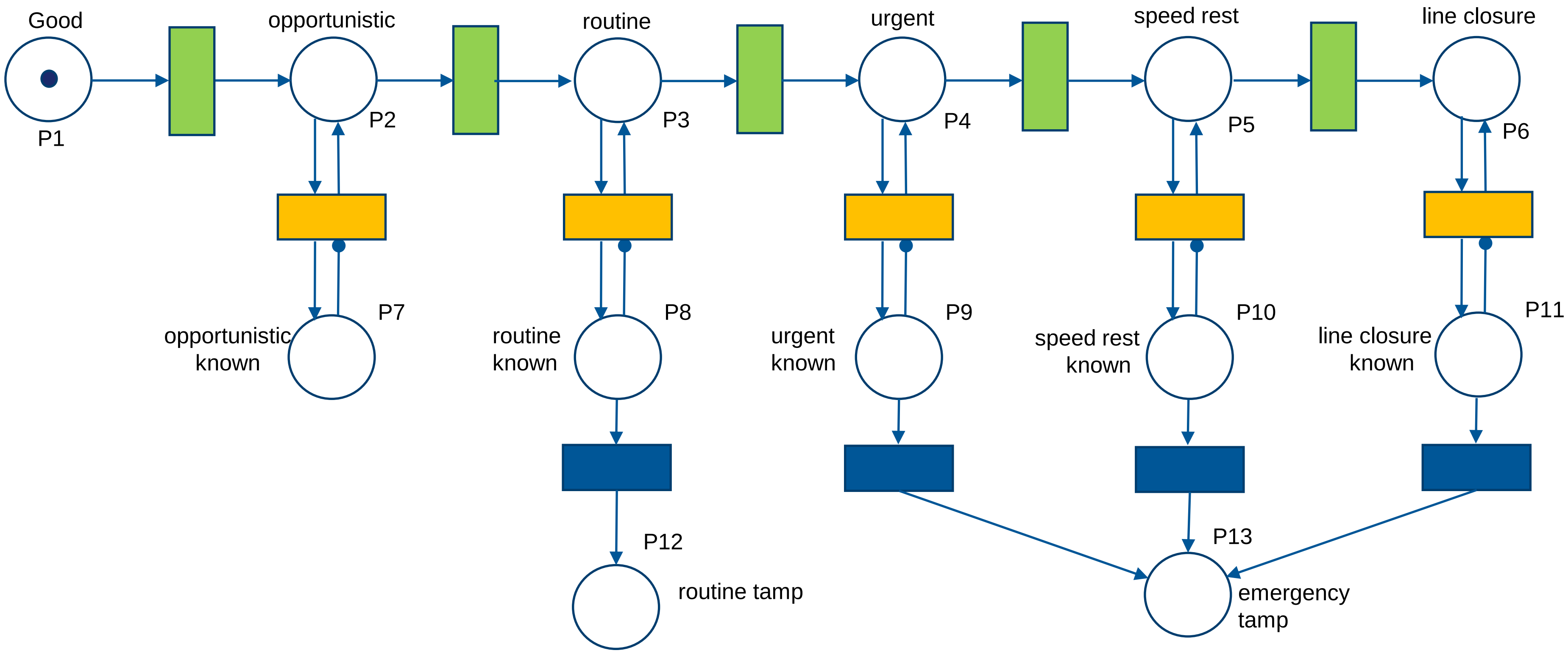
LC	Line Closure / emergency maintenance
SR	Speed Restriction / emergency maintenance
UR	Urgent Maintenance
PO	Poor Condition / Routine Maintenance
OP	Opportunistic Maintenance
GD	Good Condition



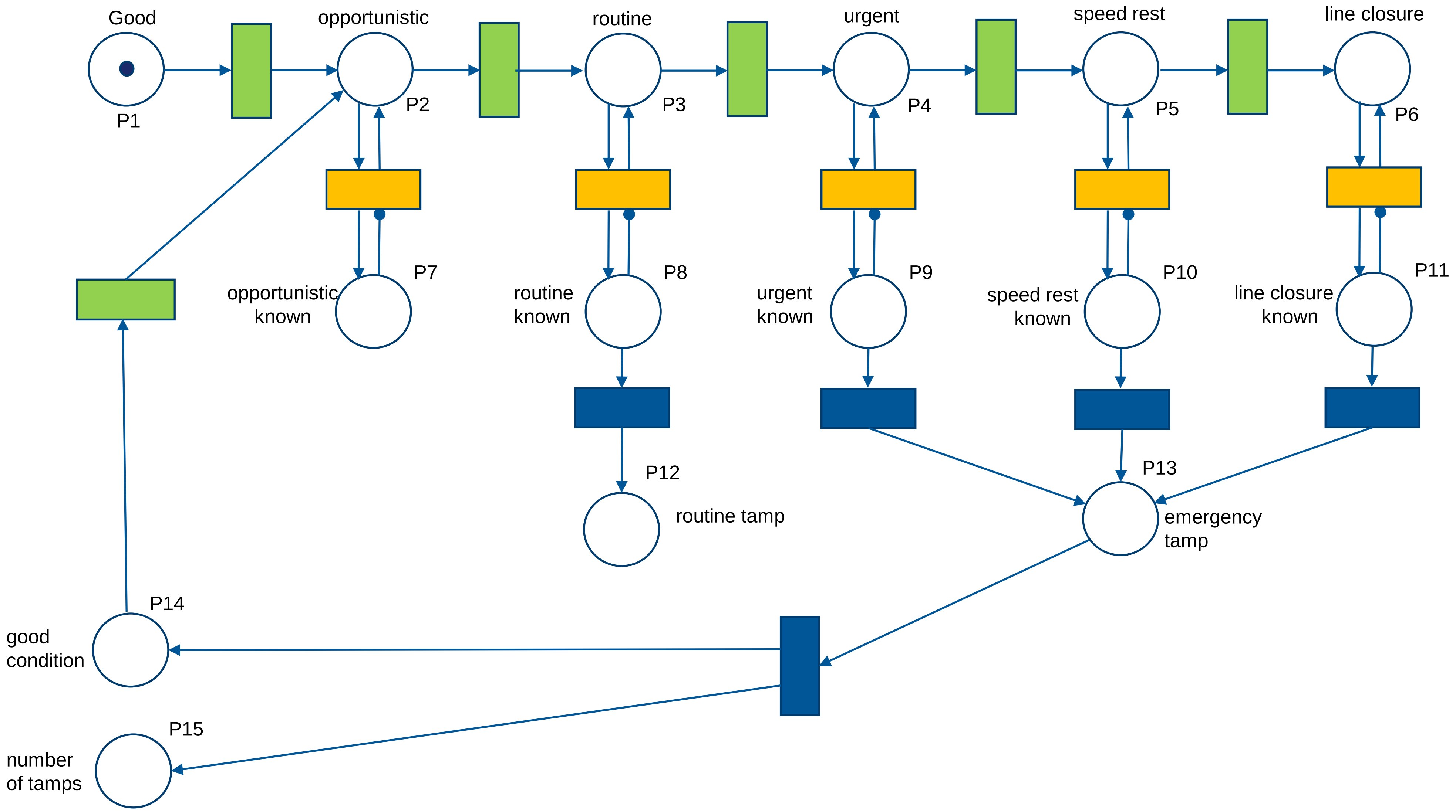
Degradation


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

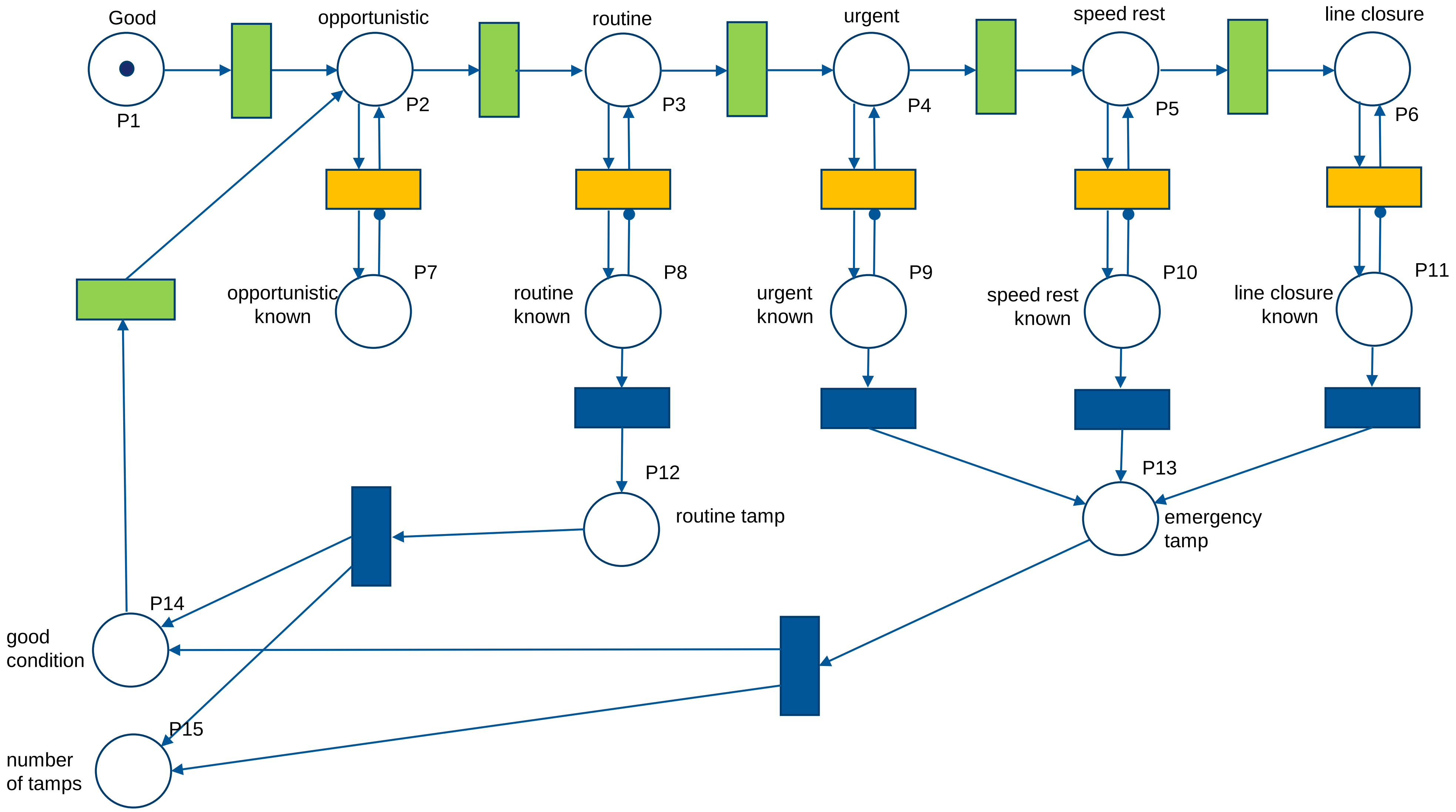
Inspection



Repair Options



Emergency Repair



Degradation time distributions account for the variation of all track sections along a route.

Routine Repair

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 %	Service disruption
	Unknown	0.0%	0.043 %	0.056 %	Potential safety issue
Line Closure needed	Known	0.0%	0.005 %	0.018 %	Service disruption
	Unknown	0.0%	0.057 %	0.07 %	Potential safety issue

Model results – Key Performance Metrics over a 30 year period

Event	Number		
	Min	Average	Max
Track Inspections	391	391	391
Routine Intervention (tamp)	0.0	3.7	12.5
Emergency Intervention (tamp)	0.0	2.58	3.11
Speed Restriction	0.0	0.2	2.3
Line Closure	0.0	0.028	1.57

University of Nottingham
UK | CHINA | MALAYSIA

Resilience Engineering

University of Nottingham
UK | CHINA | MALAYSIA

Track Buckling

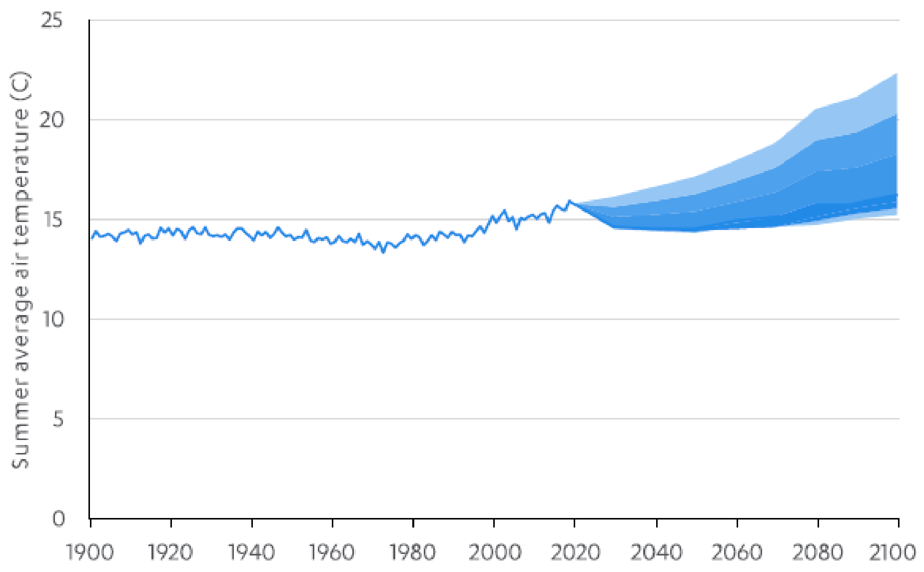
Hot Weather

Considering Climate Change

Effects of Climate Change – period of sustained high temperature

- Expansion in the rails means that tamping risks causing them to buckle.
- No tamping - causes a drift towards a poorer condition.
- Track can be in any state at the start of the heatwave.

Figure 4.1 Predicted average summer temperatures in the UK (1900 – 2100)* [125]



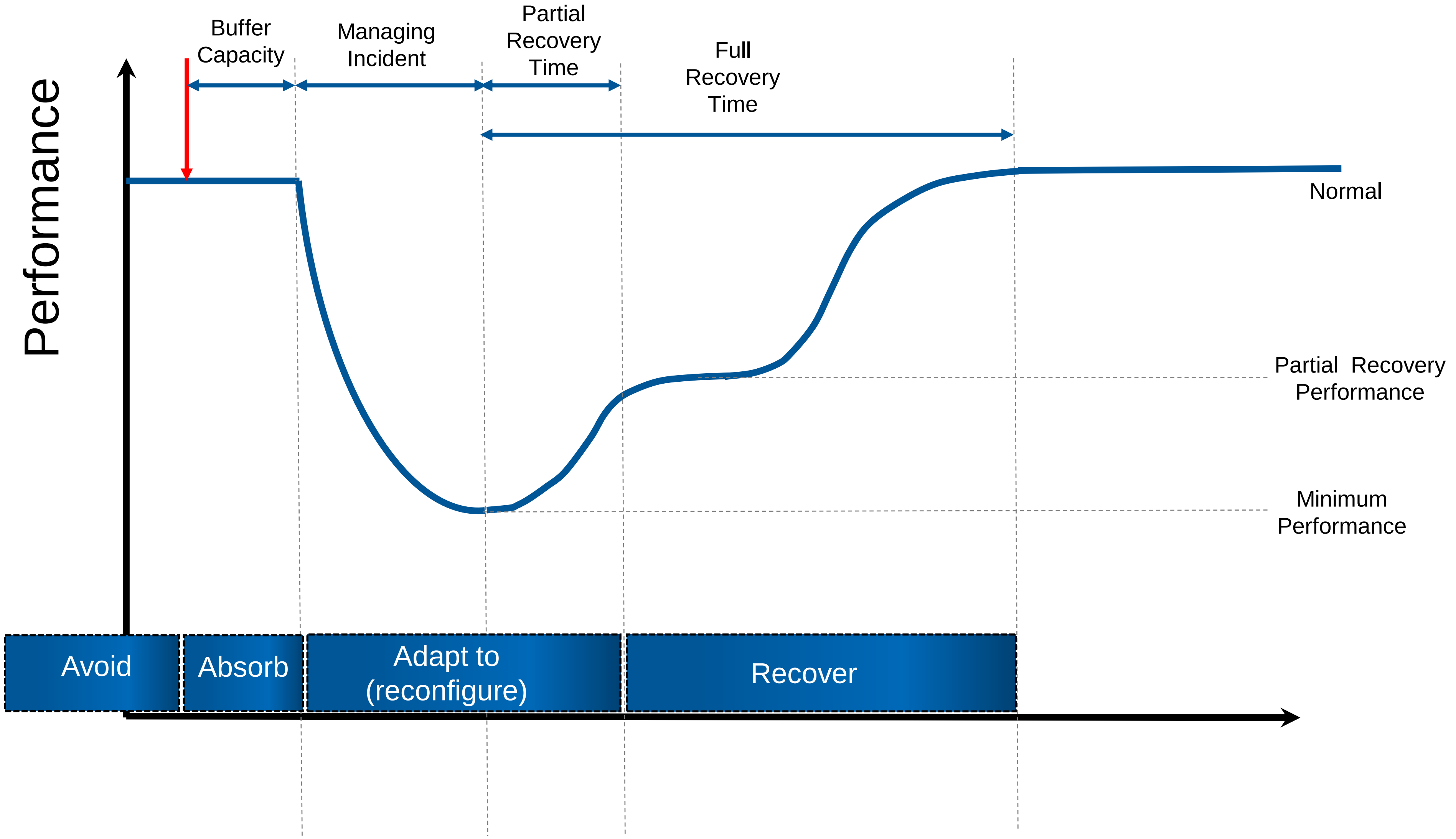
* Range of projected values based on the minimum and maximum of all UKCP18 temperature scenarios, at the 5th and 95 th percentile. Source: UKCP18

Anticipate, React, Recover, Resilient Infrastructure Systems, National Infrastructure Commission, May 2020

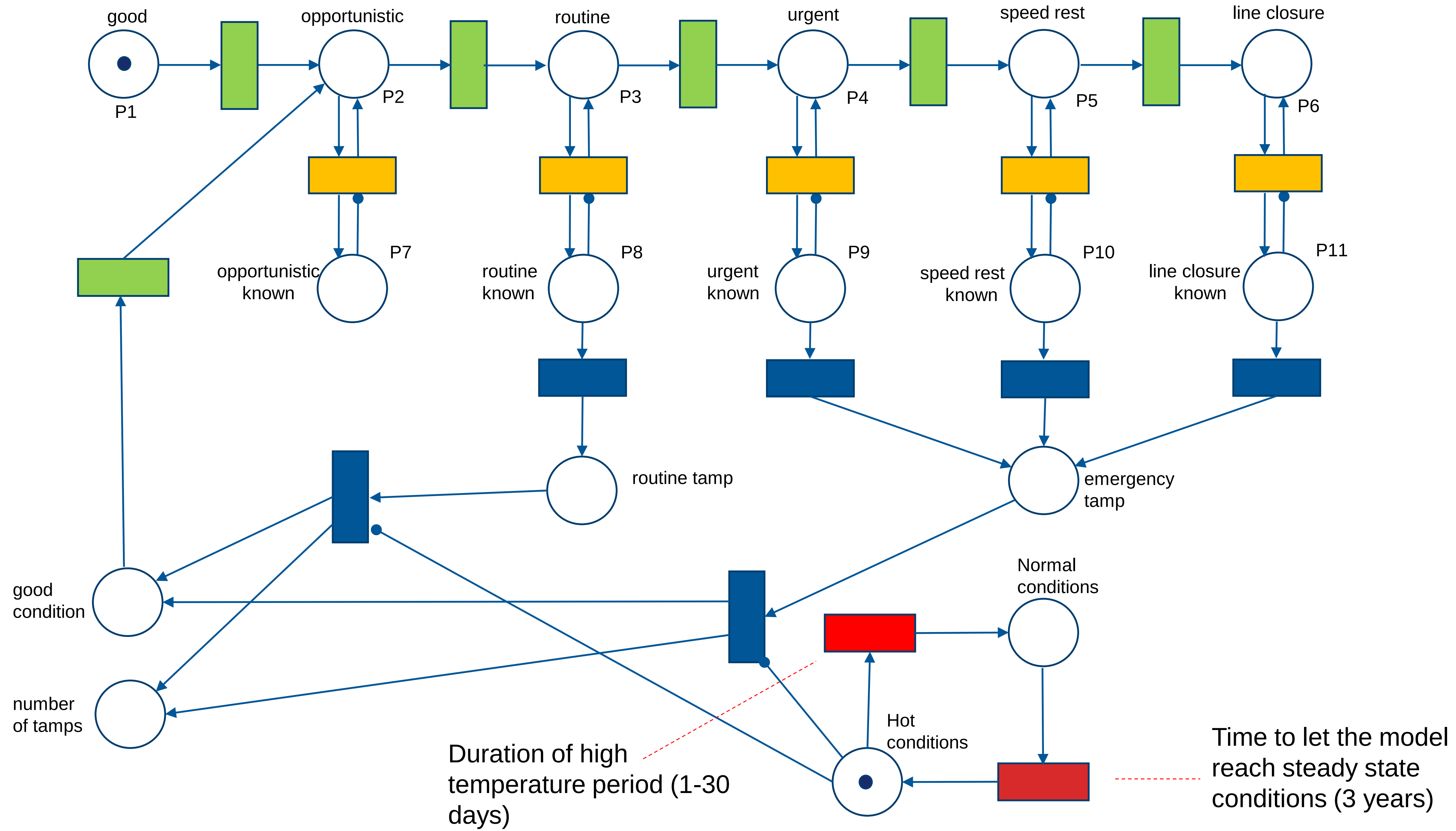
Questions

- How many days of high temperature before the risk of a safety incident or a service disruption becomes unacceptable?
- How is maintenance best performed prior to a period of high temperature to ensure geometry resilience?
- How long after the high temperature period to clear the backlog of work?

Engineering System Resilience



Modified Model – weather module



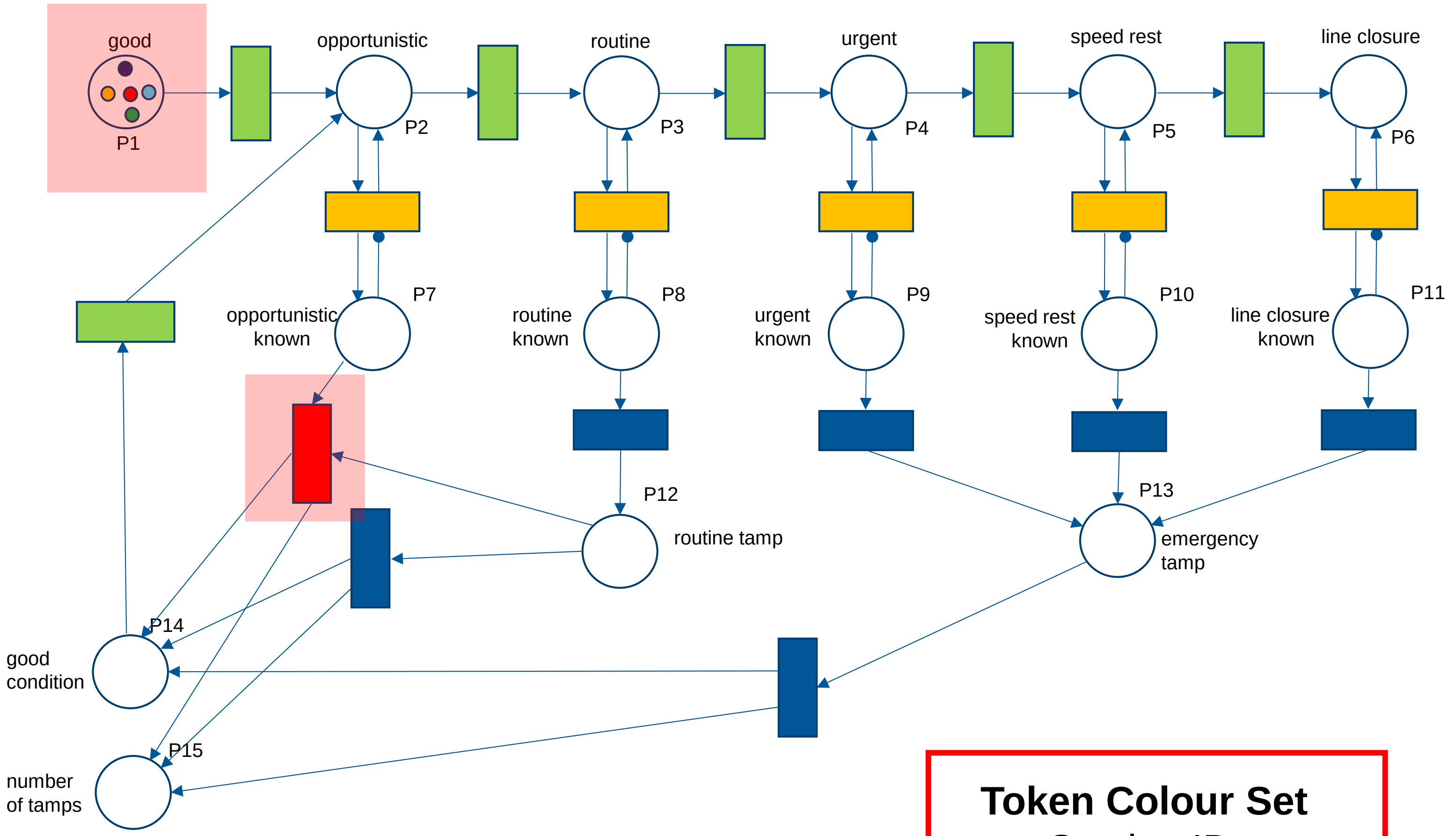
University of Nottingham
UK | CHINA | MALAYSIA

Model results – Consider a line of 160 miles

1280 track sections

Days into heatwave	Expected Number at full capacity	Expected number with speed restrictions	Expected number of line closures	Tamping backlog at end of heatwave	
				Routine	Urgent
0	1279.89	0.11	0.00	0.35	0.0
5	1279.23	0.77	0.00	2.56	2.22
10	1279.15	0.85	0.00	4.77	4.43
15	1278.89	1.11	0.00	7.26	4.45
20	1278.55	1.45	0.00	9.13	4.48
25	1278.46	1.54	0.00	11.61	4.51
30	1278.12	1.88	0.00	13.74	4.53

System / Route Model – Coloured Petri Nets



- Coloured tokens represent each section
  - localised transition parameters
  - transition times stored within the token
- Transition constantly receptive to firing.

Token Colour Set

- Section ID
- Location
- Tamping history
- Time stamp

Summary

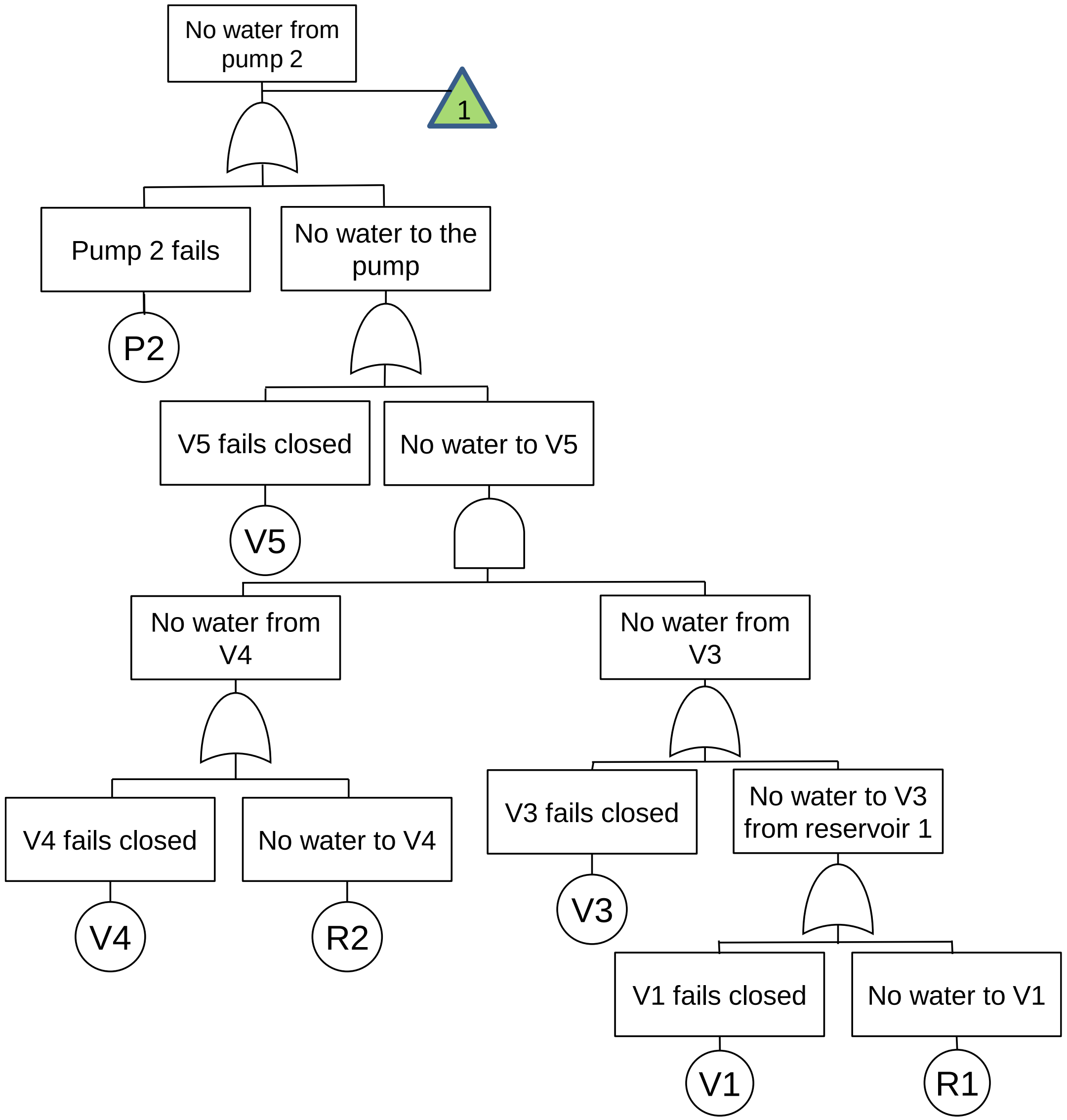
- Simple example has been used to present the capabilities of Petri Net modelling approaches to support decisions on Railway Infrastructure Resilience Modelling
- The models are incredibly flexible and capable of:
  - mimicking the maintenance processes and strategies carried out no matter how complex.
  - applicable to a broad range of applications – such as climate change.
  - extension to include different failure modes:
    - twist, horizontal alignment, cyclic top, gauge
    - rail grinding and welding
    - other forms of maintenance – stone blowing / ballast cleaning
- Can be extended to include different asset types to produce a system or a route model – allowing a system level decision process

University of Nottingham
UK | CHINA | MALAYSIA

Quantified Risk Assessment

Probabilistic Safety Assessment

Fault Tree Analysis



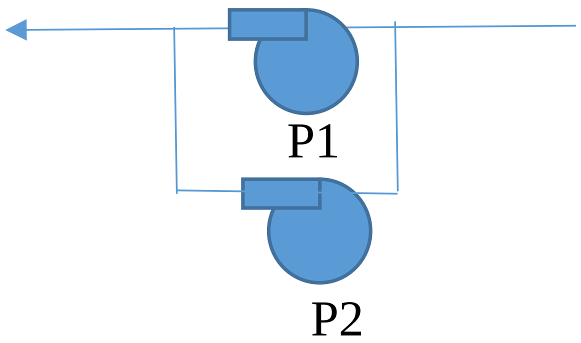
Component failure models

- 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: $Q_{AV} = \lambda\left(\frac{\theta}{2} + \tau\right)$
- Snap-shot in time

PROJECT AIMS

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

Standby Systems



Standby System

- Pump P1 operational.
- When P1 fails P2 takes over the duty

Hot Standby

Both pumps are operational but the fluid is just driven by P1. On failure of P1, the fluid now passes through P2

P1 & P2 Independent

Warm Standby

Pump P2 is not operational in standby. It becomes operational when P1 fails. It can fail in standby but with a lower rate than when operational.

P1 & P2 Dependent

Cold Standby

Pump P2 is not operational in standby. It becomes operational when P1 fails. It cannot fail in standby.

P1 & P2 Dependent

Dependency Examples

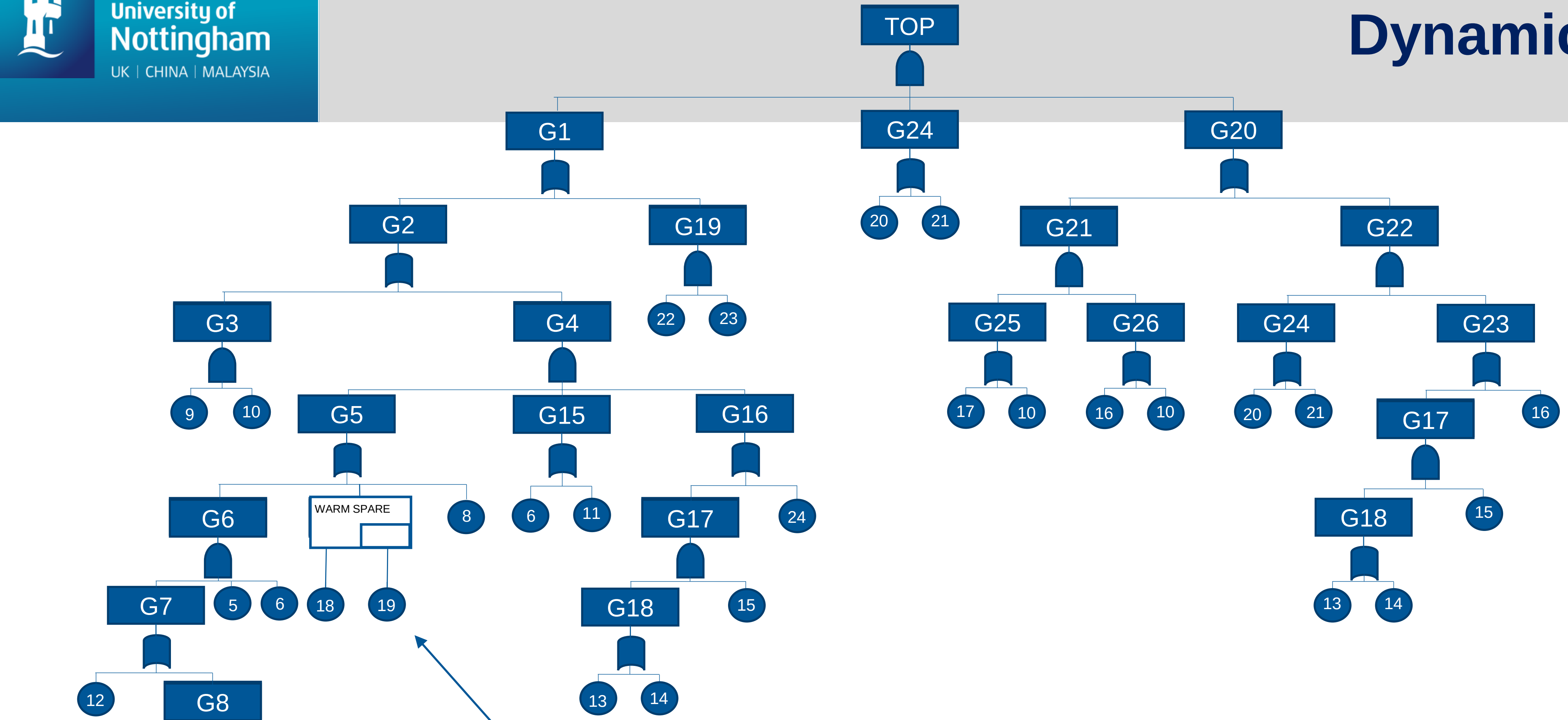
Type	Description	Example
Secondary Failure	When one component fails it increases the load on a second component which then experiences an increased failure rate	Two pumps both operational and sharing the load. Each pump has the capability to deliver the full demand should the other pump fail
Opportunistic Maintenance	A component fails which causes a system shutdown or the requires specialist equipment for the repair. The opportunity is taken to do work on a second component which has not failed but is in a degraded state	Components on a circuit board. Components in a sub-sea production module
Common Cause	When one characteristic (eg materials, manufacturing, location, operation, installation maintenance) causes the degraded performance in several components	Incorrect maintenance done on several identical sensors Impact breaks the circuit on cables routed in the same way to different redundant channels
Queueing	Failed components all needing the same maintenance resource are queued. Then repaired in priority order	Limited number of maintenance teams, equipment or spares

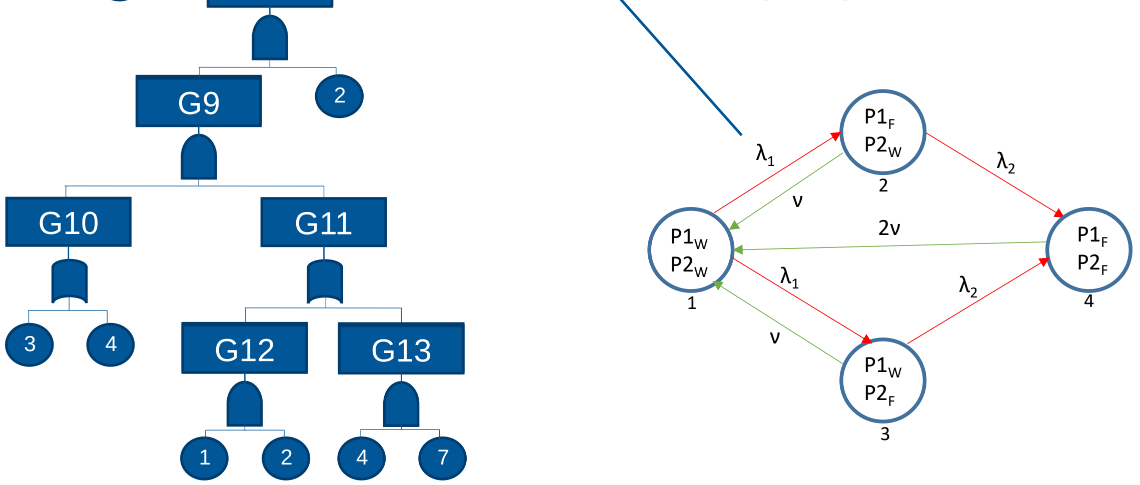
University of Nottingham
UK | CHINA | MALAYSIA

Dynamic & Dependent Tree Theory (D^2T^2)

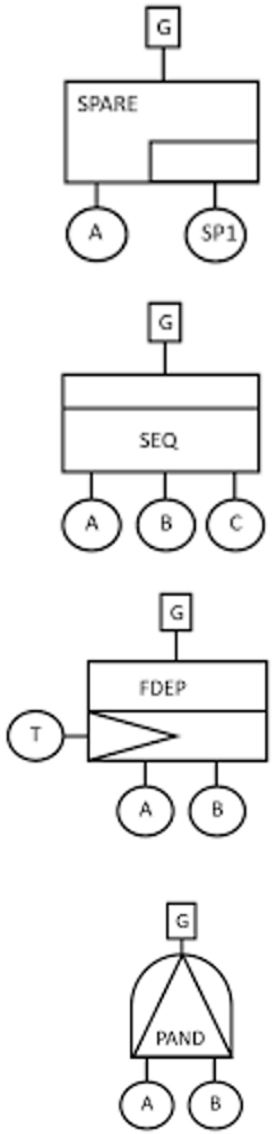
A Fault Tree Analysis Framework

Dynamic Fault Trees

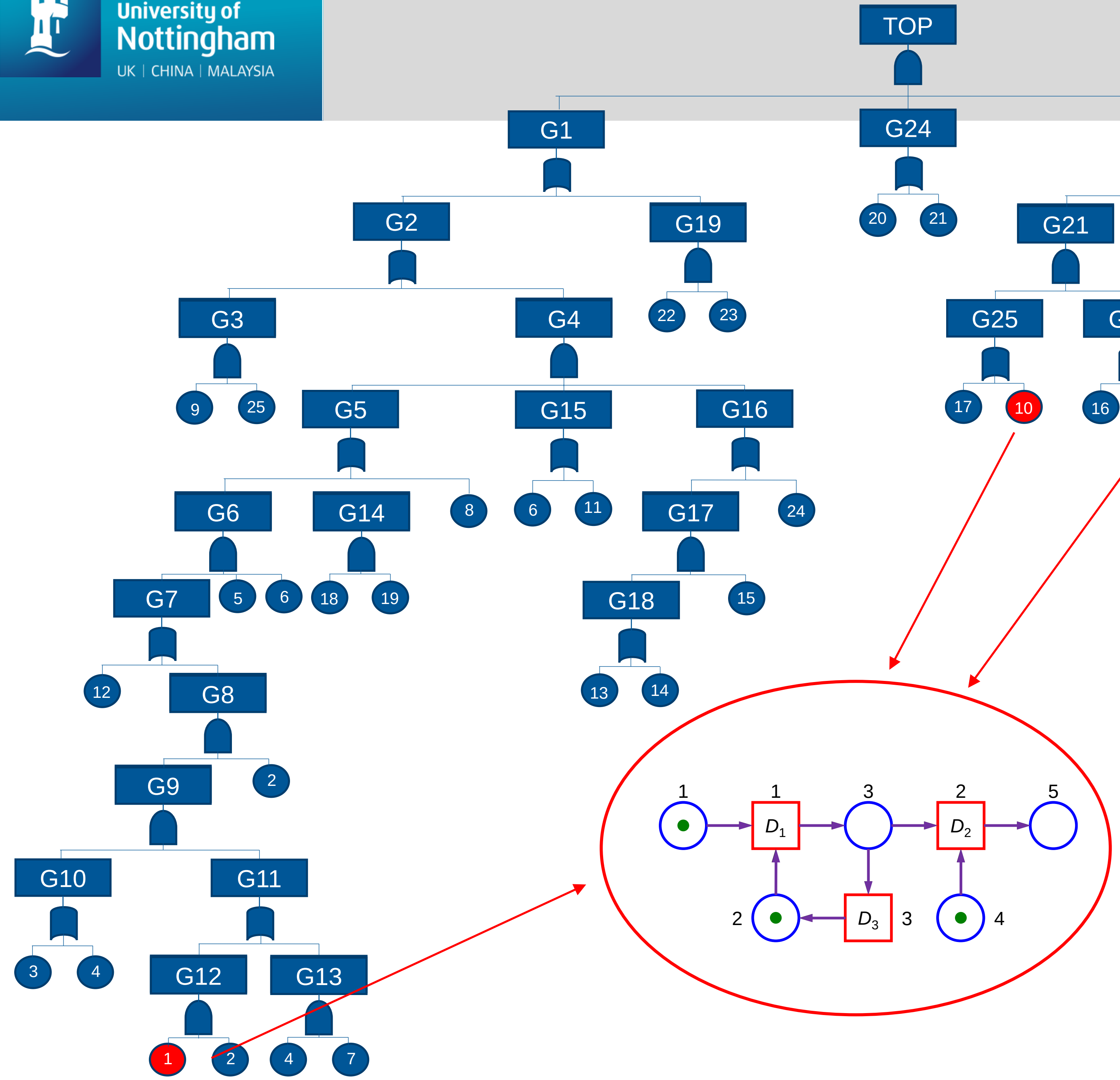


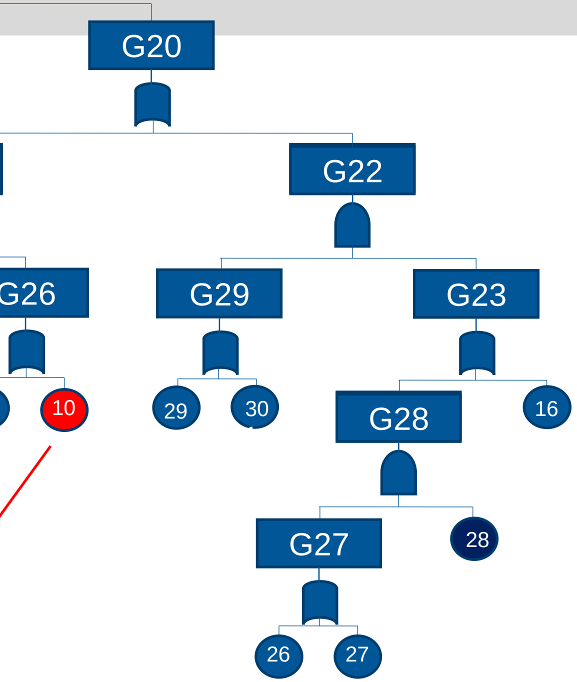


- Difficulties if events 18 or 19 appear elsewhere in the FT



Independent Modules





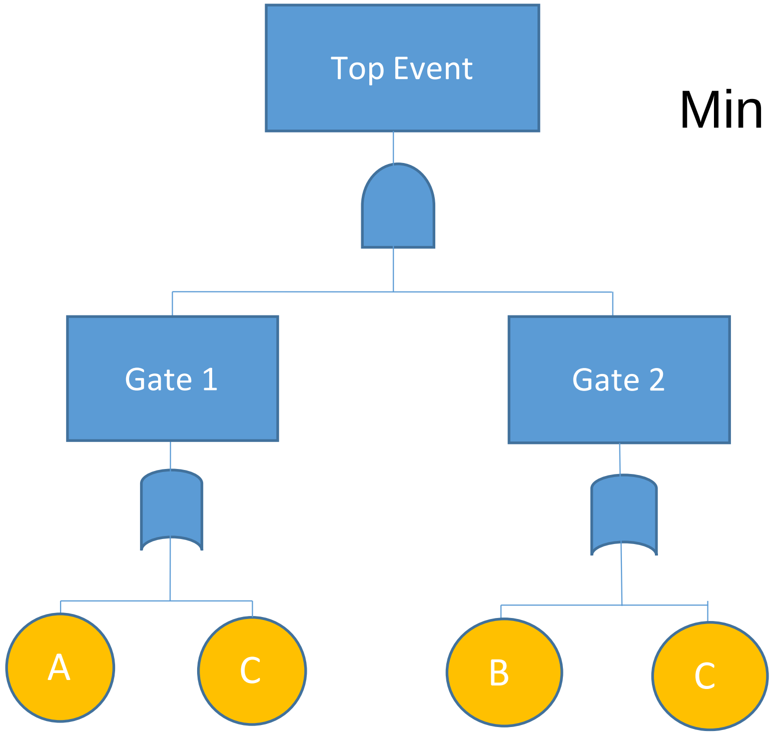
Maintenance dependency's can affect events which are not geographically close in the FT structure

Small model containing only the dependent events

Integration of Fundamental Quantification Methodologies

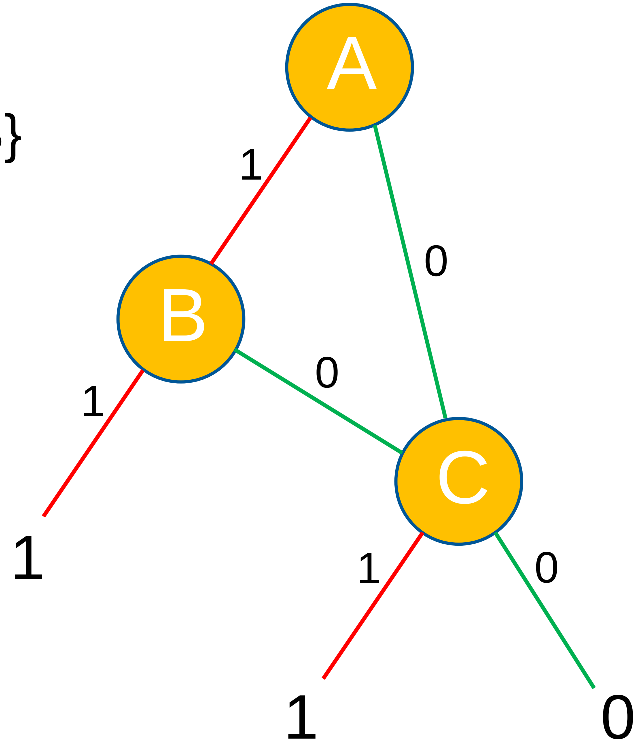
Fault Tree Analysis => Binary Decision Diagrams (BDD)
Petri Nets
Markov Methods

Binary Decision Diagrams – Top Event Probability



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

ORDERING A < B < C



\+ OR

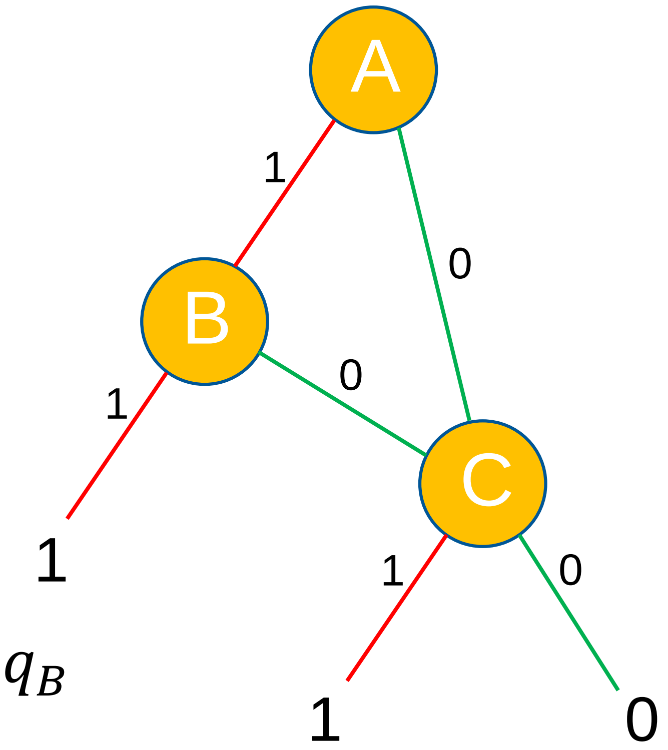
. AND

$$TOP = A.B + C$$

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

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

Binary Decision Diagrams – Top Event Probability



$q_A \, q_B$

$q_A(1 - q_B)q_C$
$+(1 - q_A) \, q_C$

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

- Exact
- Fast
- Efficient

} No need to derive the Min Cut Sets as an intermediate step

***** Disjoint paths to failure *****

Approach

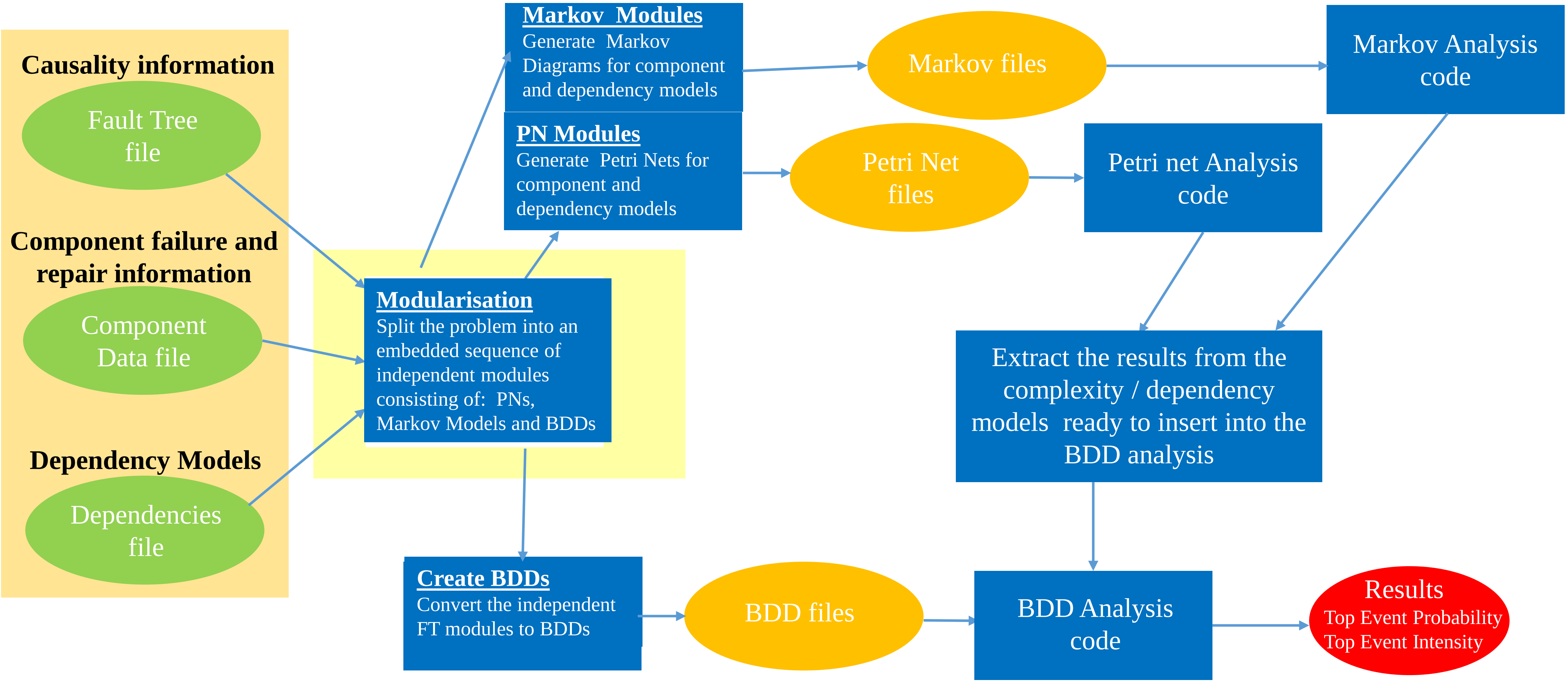
Dependencies

- Model the dependencies and complexities using Petri Nets or Markov models
  - Always use the *simplest dependency model*

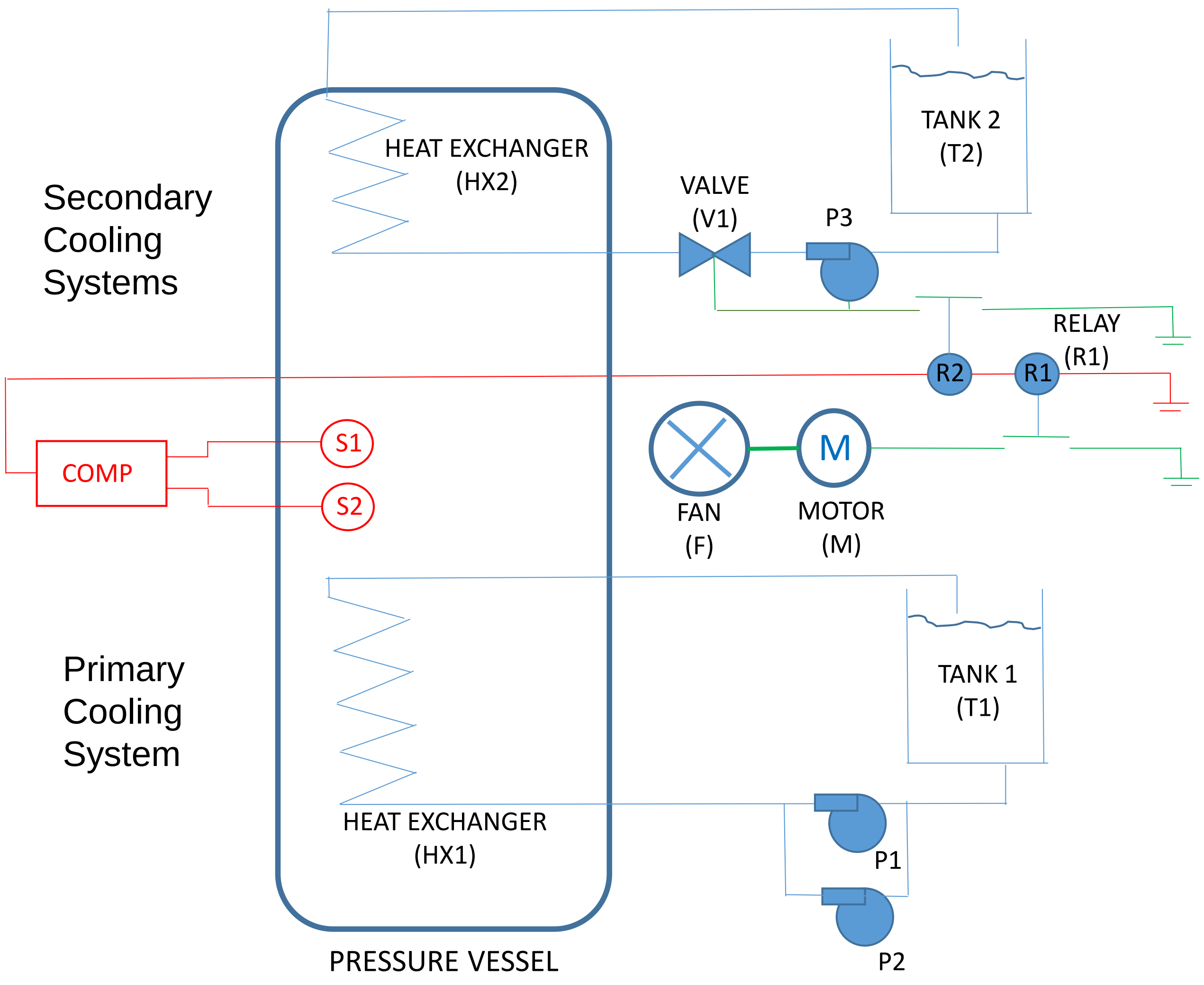
Binary Decision Diagrams

- Dependencies are just required to be considered on each path
- Path numbers can be very high so every effort needs to be made to *minimise the size of the BDD*
  - minimise the fault tree size using an effective modularisation
  - effective variable ordering

Basic Structure of the Code



Plant Cooling System and Features

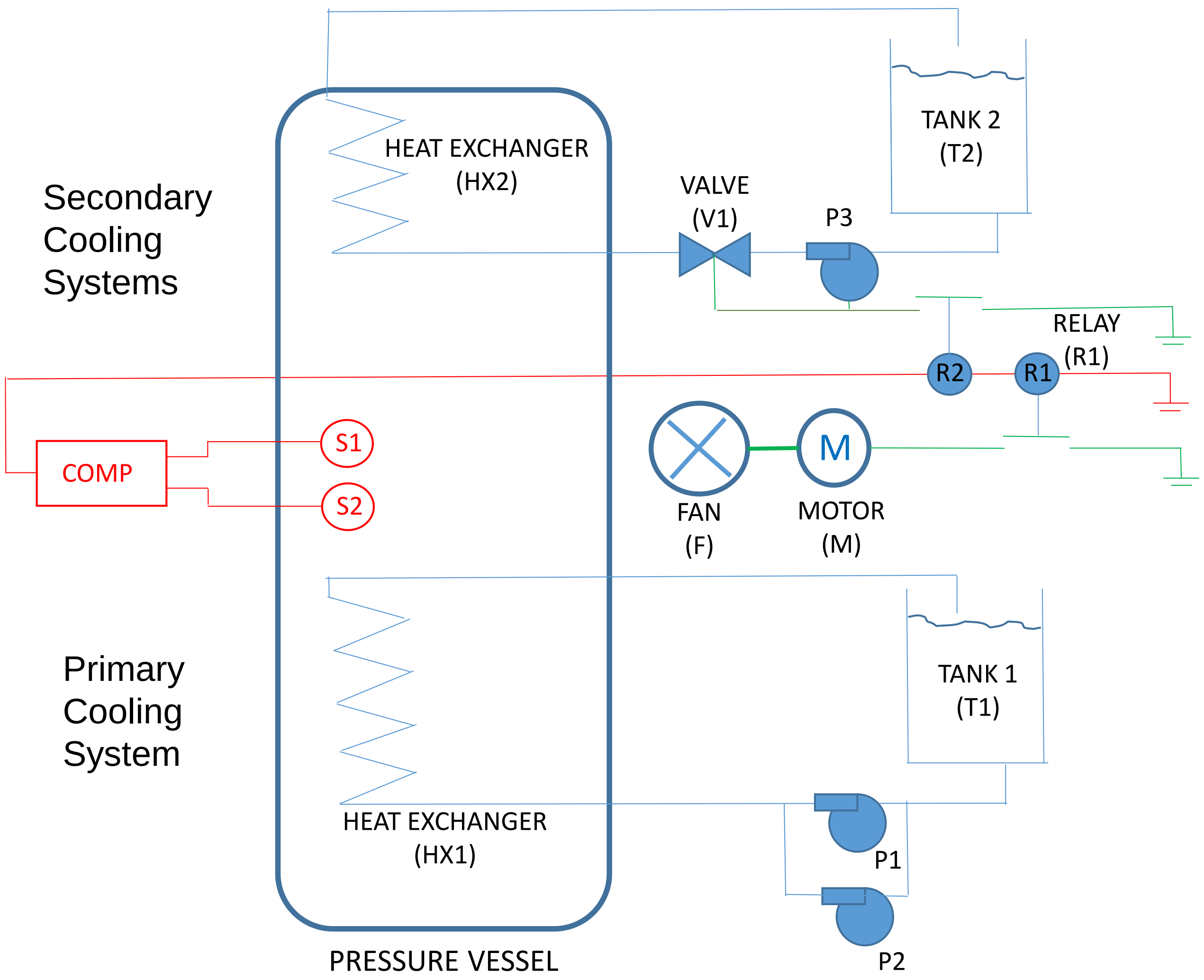


Power supply to all pumps and the valve – B1

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



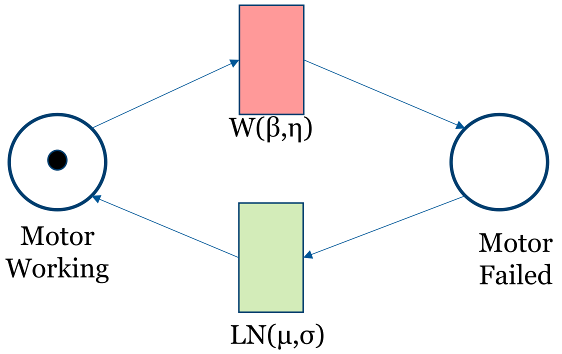
Power supply to all pumps and the valve – B1

Complex Features

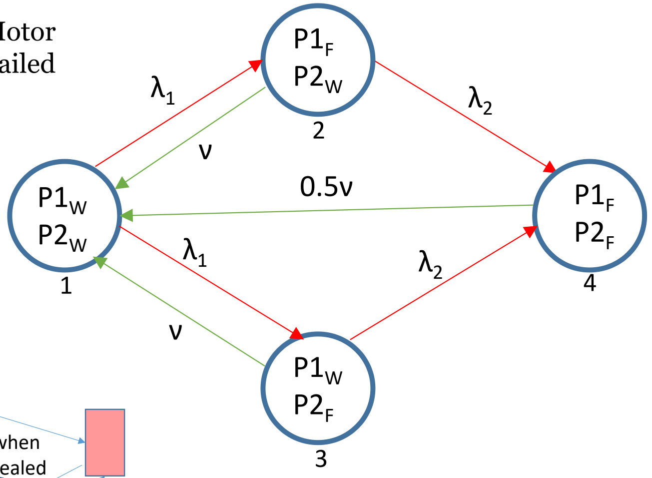
- Non-constant failure / repair rates
  - Motor M - Weibull failure time distribution and a lognormal repair time distribution
- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other
  - Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced
  - Pump P3 - two events P3S and P3R are clearly dependent

Complexity and Dependency Models

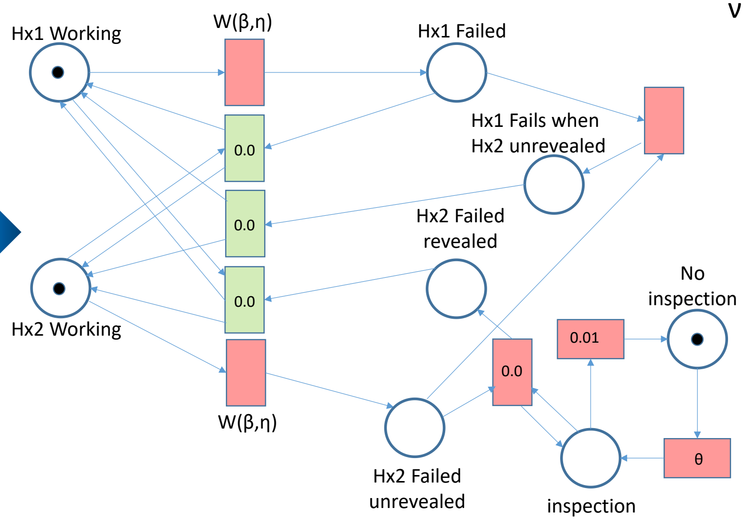
- Non-constant failure / repair rates
  - Motor M - Weibull failure time distribution and a lognormal repair time distribution



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



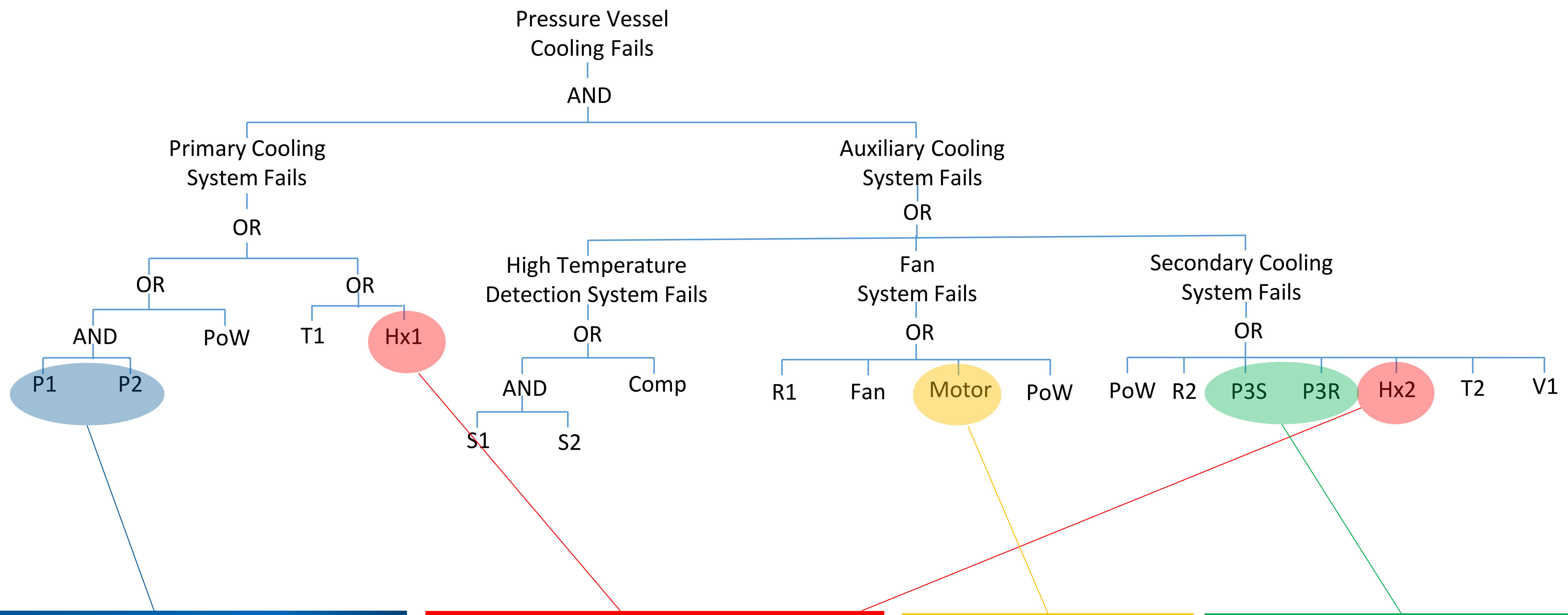
  - Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced



  - Pump P3 - two events P3S and P3R are clearly dependent

$$q_{P3} = q_{P3S} + (1.0 - q_{P3S})\lambda_{P3R}t_{period}$$
$$= 0.05 + 0.095 \times 10^{-4} \times 30$$
$$= 0.05285$$

Fault Tree Structure and Dependent Events



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

Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced

Non-constant failure / repair rates

Pump P3 - two events P3S and P3R are clearly dependent

Modularisation - Faunet

- Contraction

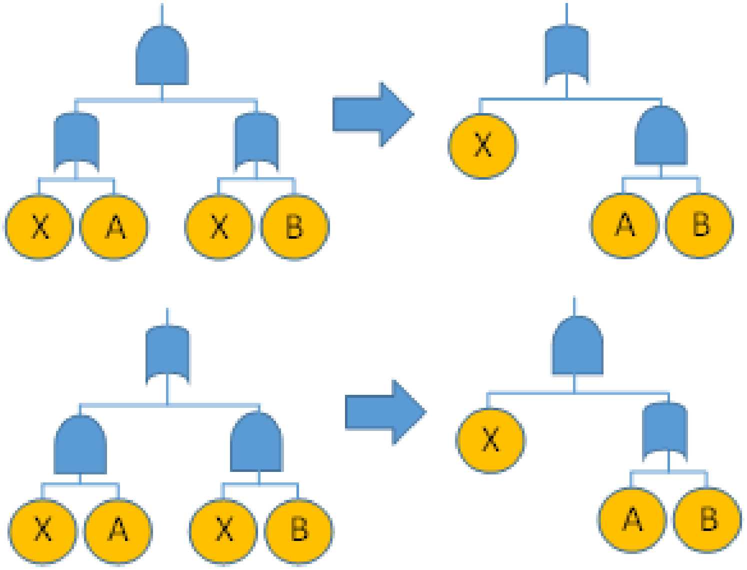
  Subsequent gates of the same type are contracted into a single gate

- Factorisation

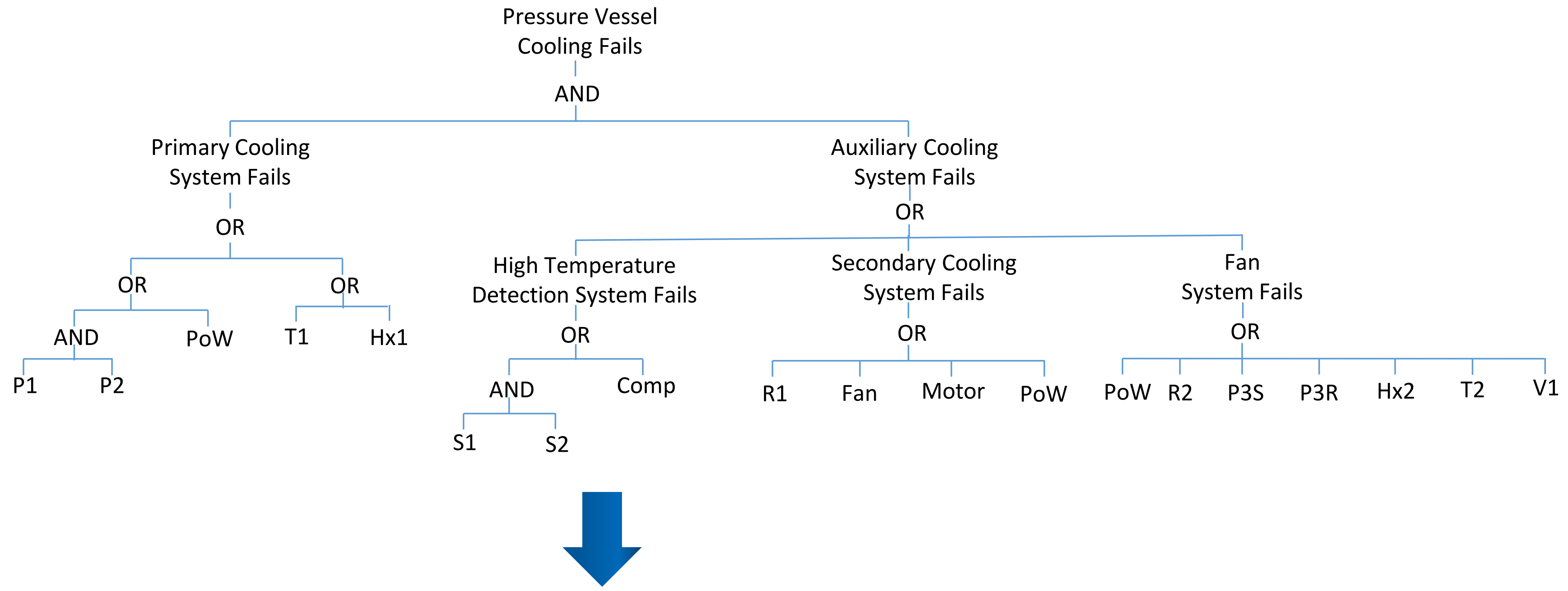
  Extracts factors expressed as groups of events that always occur together in the same gate type. The factors can be any number of events if they satisfy the following:
  - All events in the group are independent and initiators
  - All events in the group are independent and enablers.
  - All events in the group feature a dependency and contain all events in the same dependency group.

- Extraction

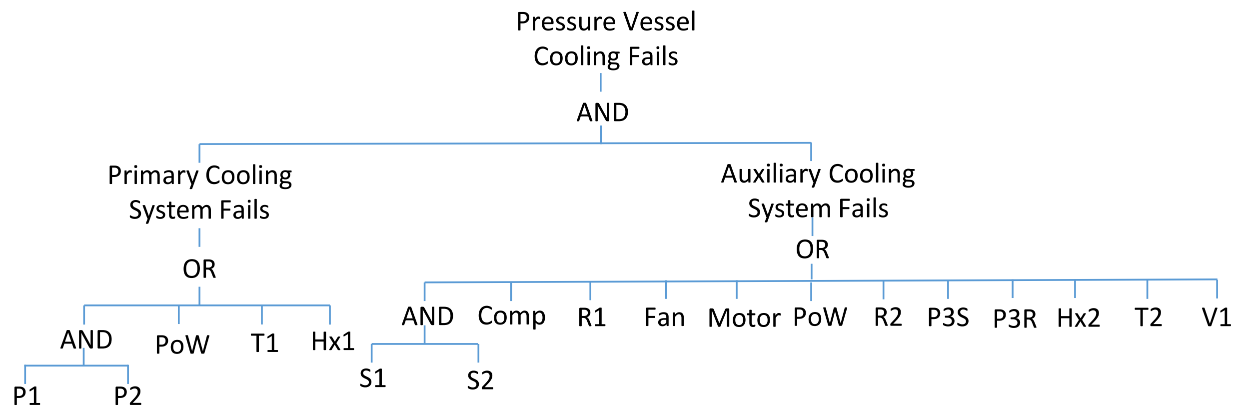
  Restructure:



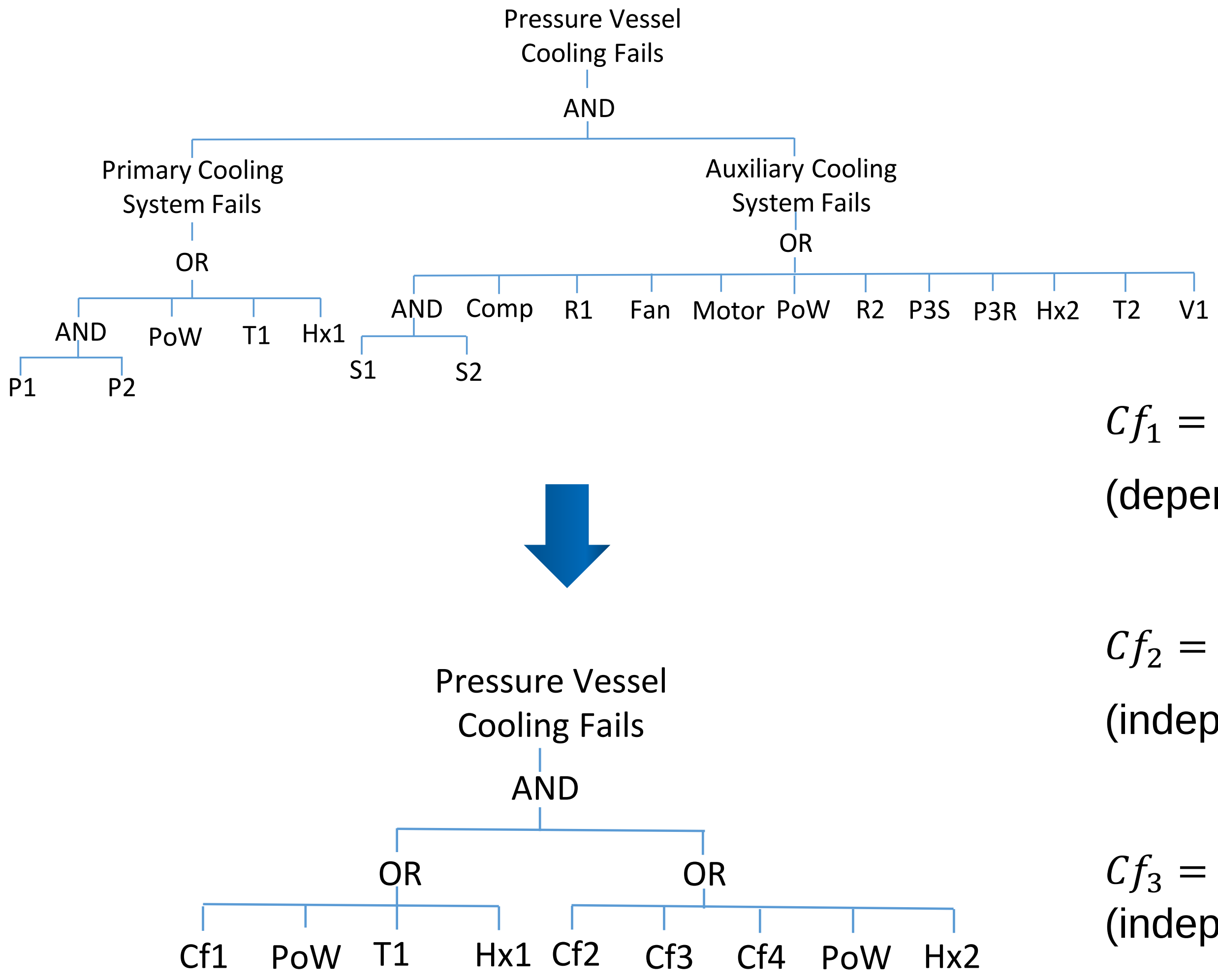
Modularisation (1)



Contraction 1



Modularisation (2)



Factorise 1

$Cf_1 = P1.P2$

(dependency group D1 – initiators)

$Cf_2 = S1.S2$

(independent enablers)

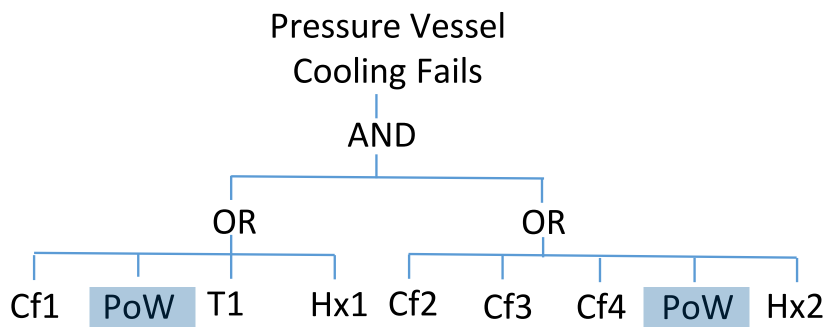
$Cf_3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$

(independent enablers)

$Cf_4 = P3S + P3R$

(dependency group D3 – enablers)

Modularisation (3)



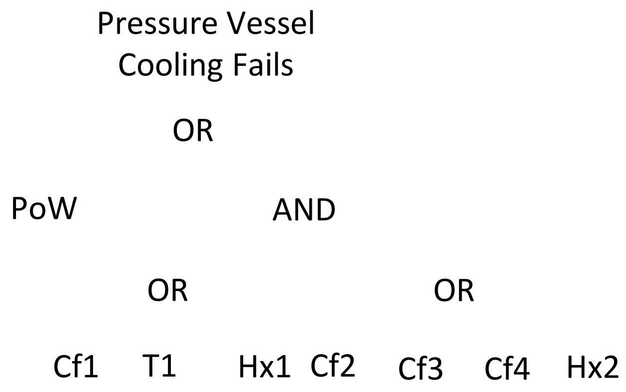
$$Cf_1 = P1.P2$$

$$Cf_2 = S1.S2$$

$$Cf_3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$$

$$Cf_4 = P3S + P3R$$

Extract 1



Contraction 2 -- No change

Modularisation (4)

Pressure Vessel
Cooling Fails

OR

PoW AND

OR OR

Cf1 T1 Hx1 Cf2 Cf3 Cf4 Hx2

$$Cf_1 = P1.P2$$

$$Cf_2 = S1.S2$$

$$Cf_3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$$

$$Cf_4 = P3S + P3R$$

Factorise 2

Pressure Vessel
Cooling Fails

OR

PoW AND (G1)

OR OR

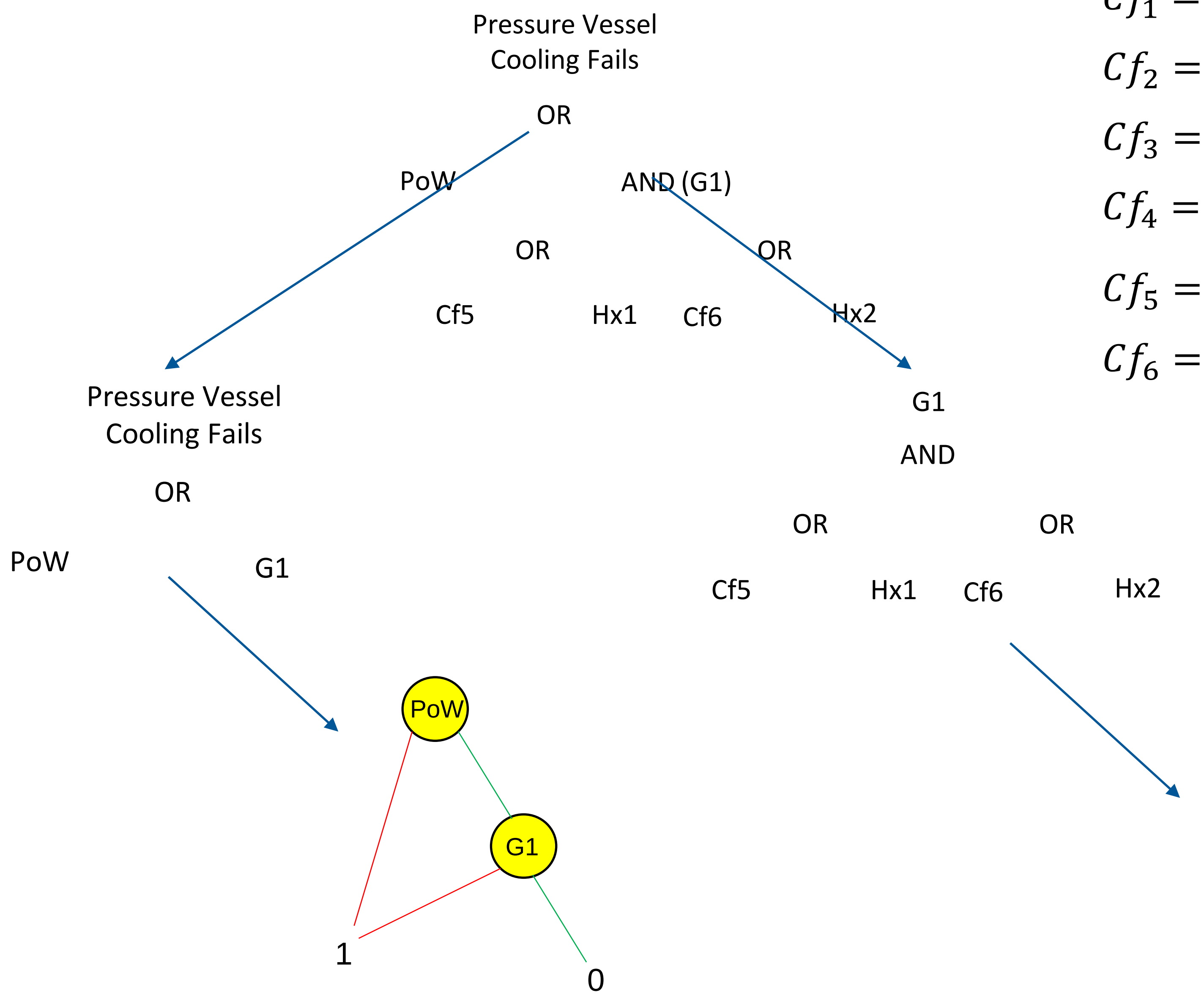
Cf5 Hx1 Cf6 Hx2

$$Cf_5 = Cf_1 + T1$$

$$Cf_6 = Cf_2 + Cf_3 + Cf_4$$

Simplest possible Faunet representation

Modularisation (5) - Rauzy & Dutuit



$$Cf_1 = P1.P2$$

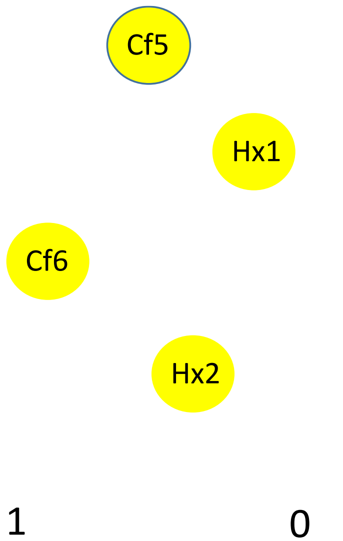
$$Cf_2 = S1.S2$$

$$Cf_3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$$

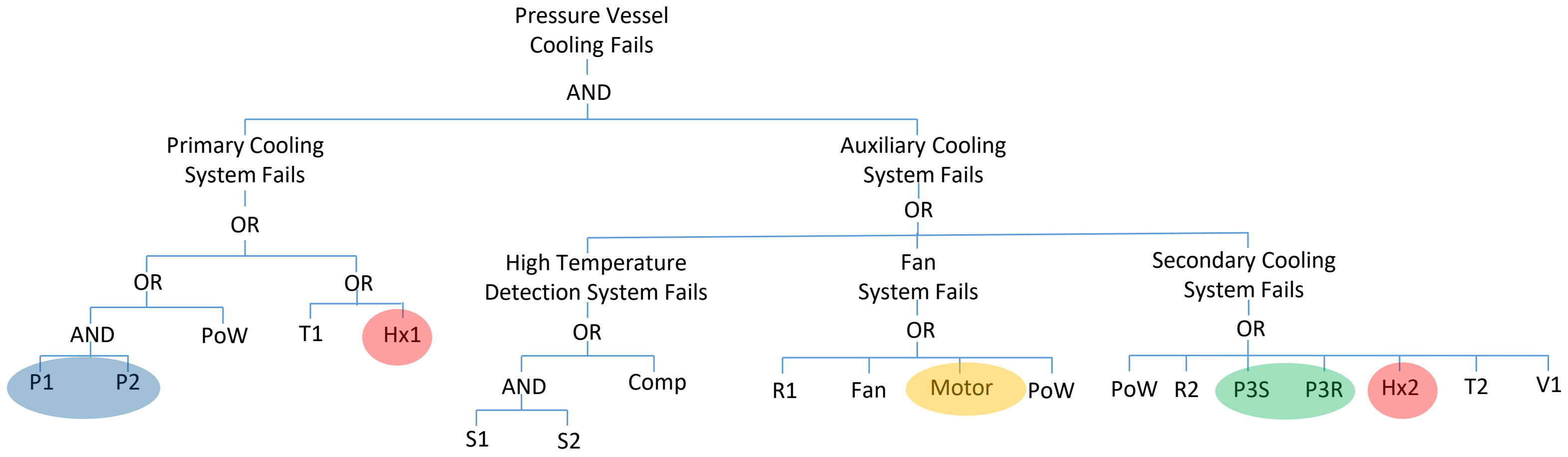
$$Cf_4 = P3S + P3R$$

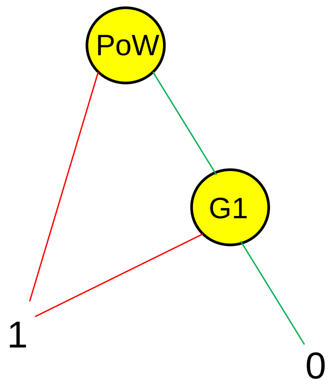
$$Cf_5 = Cf_1 + T1$$

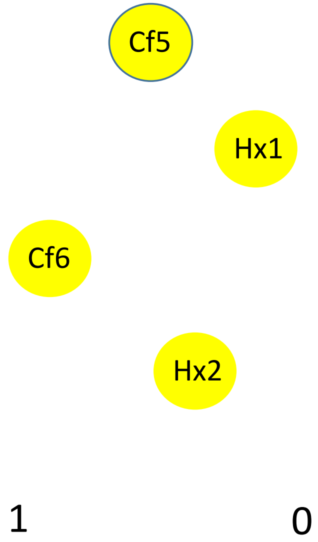
$$Cf_6 = Cf_2 + Cf_3 + Cf_4$$



Modularisation







$$Cf_1 = P1.P2$$

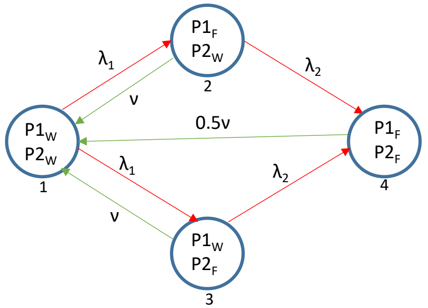
$$Cf_2 = S1.S2$$

$$Cf_3 = Comp + R1 + Fan$$
$$+ Motor + R2 + T2 + V1$$

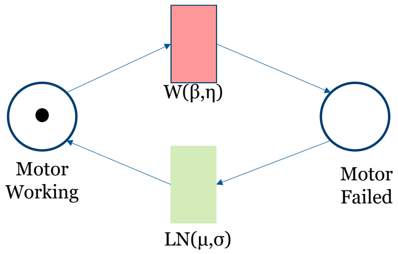
$$Cf_4 = P3S + P3R$$

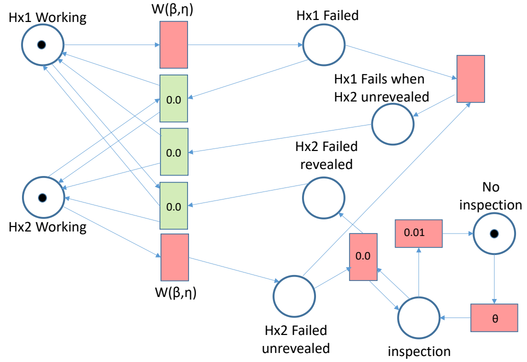
$$Cf_5 = Cf_1 + T1$$

$$Cf_6 = Cf_2 + Cf_3 + Cf_4$$

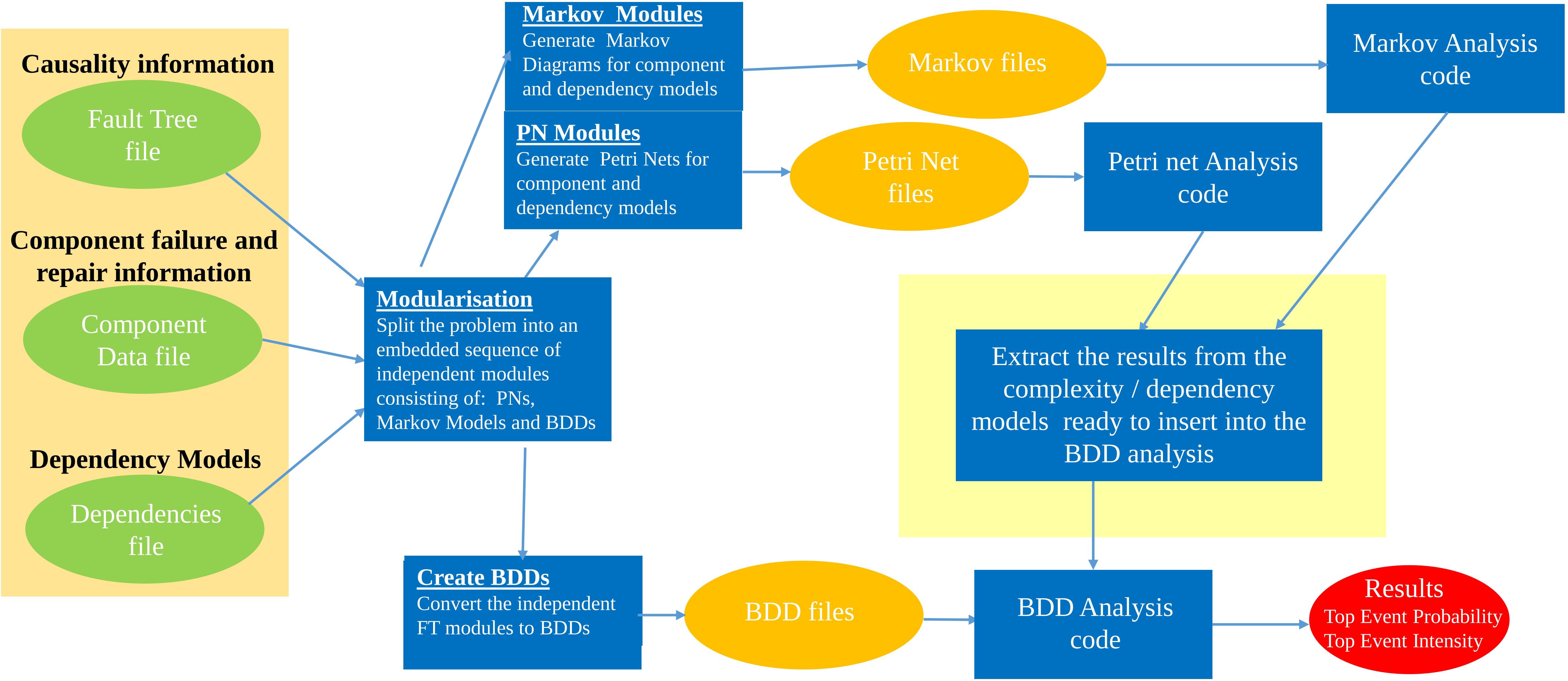


$$q_{Cf3} = q_{P3S} + (1.0 - q_{P3S})\lambda_{P3R}t_{period}$$

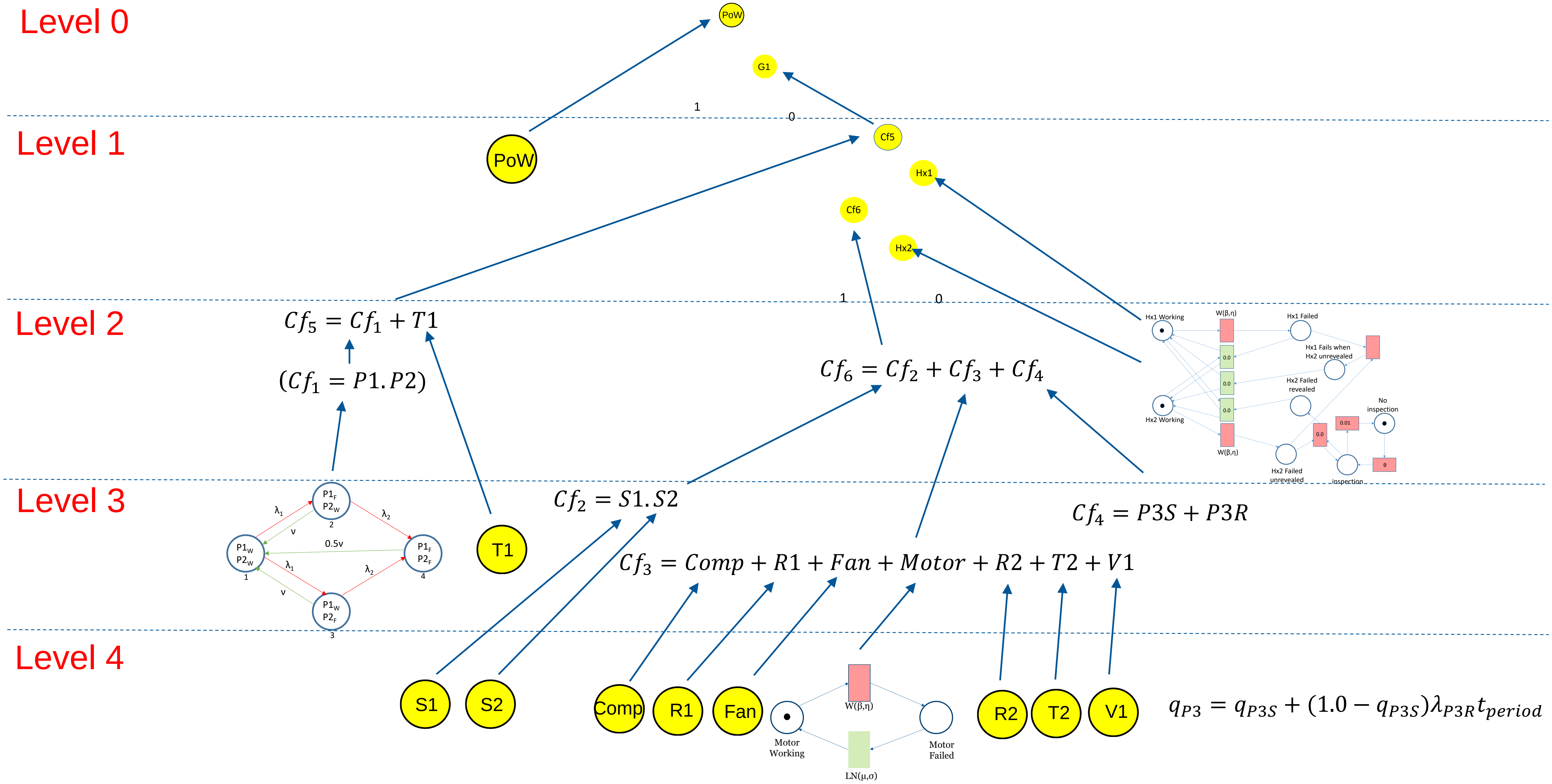




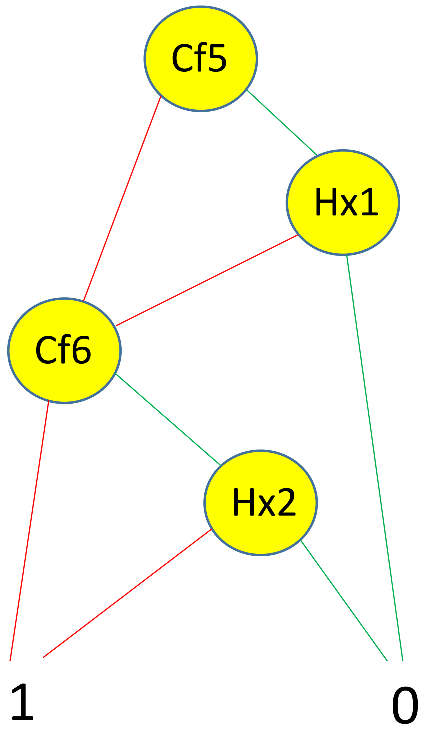
Basic Structure of the Code



Integration



Integration



j	$path_j$	$Ipath_j$	$Dpath_j^1$
1	$Cf5_1, Cf6_1$	$Cf5_1, Cf6_1$	
2	$Cf5_1, Cf6_0, Hx2_1$	$Cf5_1, Cf6_0$	$Hx2_1$
3	$Cf5_0, Hx1_1, Cf6_1$	$Cf5_0, Cf6_1$	$Hx1_1$
4	$Cf5_0, Hx1_1, Cf6_0, Hx2_1$	$Cf5_0, Cf6_0$	$Hx1_1, Hx2_1$

$$Q_{G1} = \sum_{j=0}^{npath} \left[P(Ipath_j). \prod_{k=1}^{ndep} P(Dpath_j^k) \right]$$

$$Q_{path1} = P(Cf5_1).\, P(Cf6_1) = 0.0010830$$

$$Q_{path2} = P(Cf5_1).\, (1 - P(Cf6_1)).\, P(Hx2_1) = 8.8052957 \times 10^{-6}$$

$$Q_{path3} = (1 - P(Cf5_1)).\, P(Cf6_1).\, P(Hx1_1) = 0.0$$

$$Q_{path4} = (1 - P(Cf5_1)).\, (1 - P(Cf6_1)).\, P(Hx1_1, Hx2_1) = 0.0$$

$$Q_{G1} = 0.00109175$$

Full FTA Features

- Top Event Frequency Calculations
- Qualitative FTA – remains unchanged
- Importance measures
- Large FTA calculations
- Event Tree Analysis

Summary

- Dynamic and Dependent Tree Theory, D^2T^2, enables the evaluation of fault trees which are not limited by the restrictions which apply to conventional fault trees solved by Kinetic Tree Theory.

- Retains the familiar and popular fault tree causality structure.

- Utilises BDDs, Petri Nets and Markov Models.

- The Petri net and Markov models dedicated to solve the complexities and dependencies are minimal in size.

- Modularisation of the fault tree minimises the size of the BDD utilised in the system evaluation (and therefore the number of paths).

Thank you for listening – any questions ?

Professor John Andrews
Faculty of Engineering
University of Nottingham

john.andrews@nottingham.ac.uk