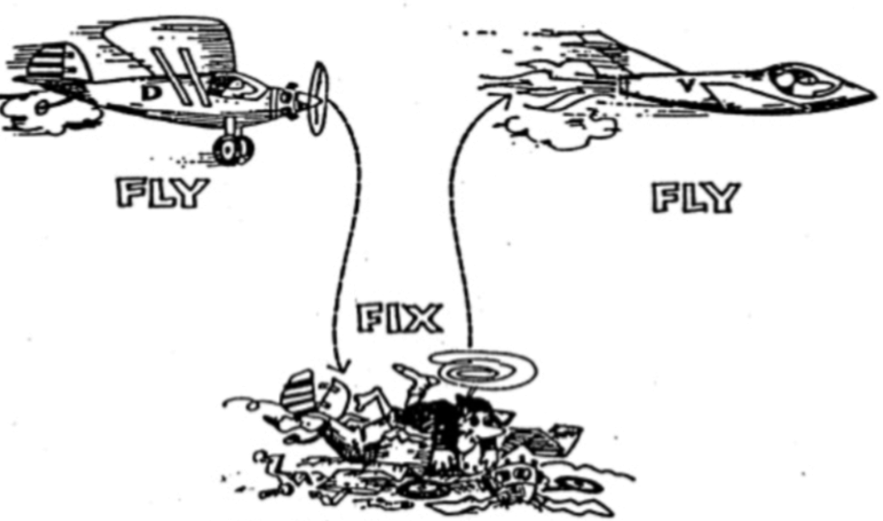
University of Nottingham
UK | CHINA | MALAYSIA

The Safety and Reliability Society
2022 Webinar Programme
26th April 2022

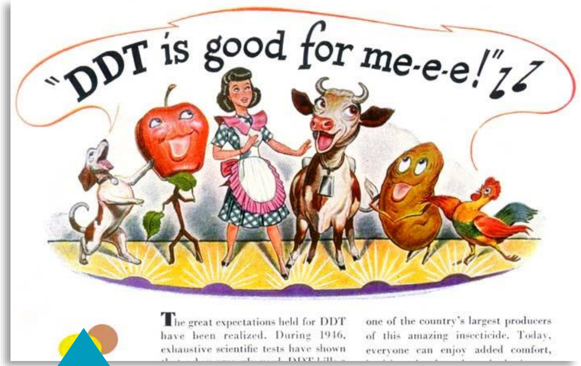
Current challenges and future solutions for system safety analysis

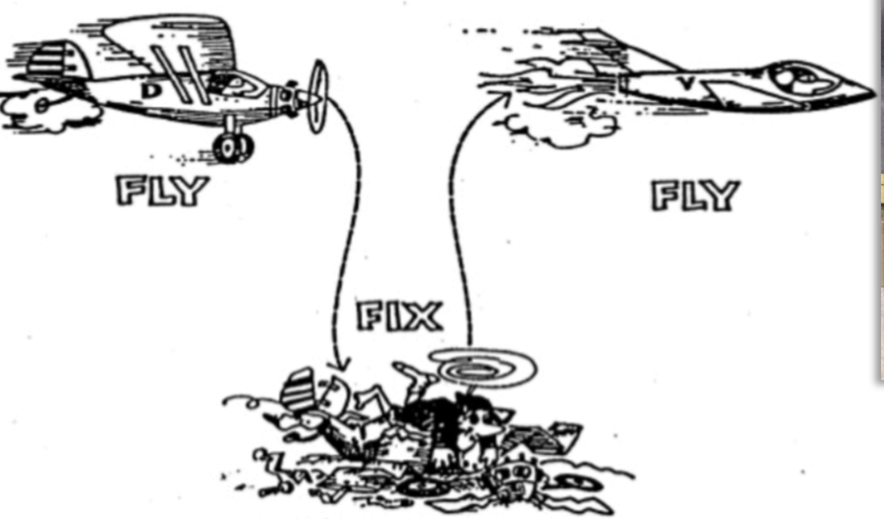
Dr Silvia Tolo

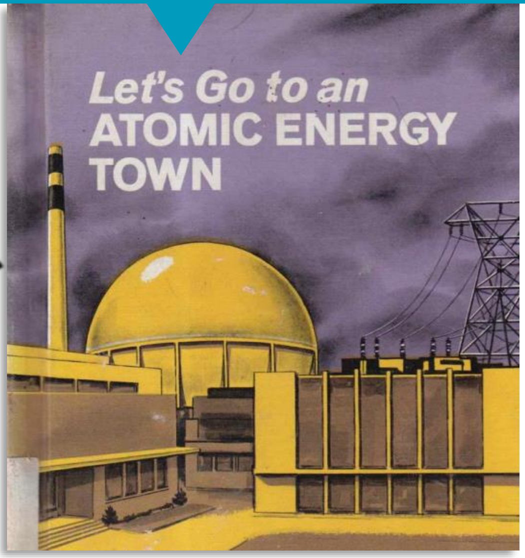
System Safety before System Safety



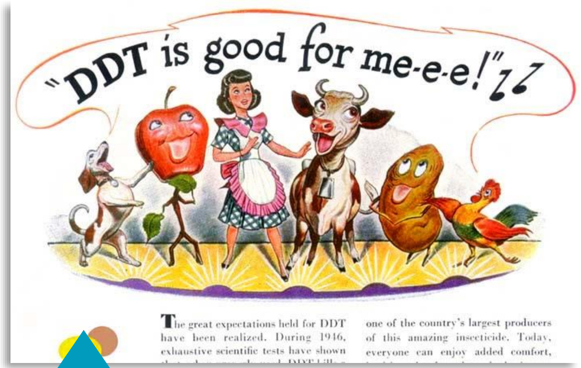
System Safety before System Safety

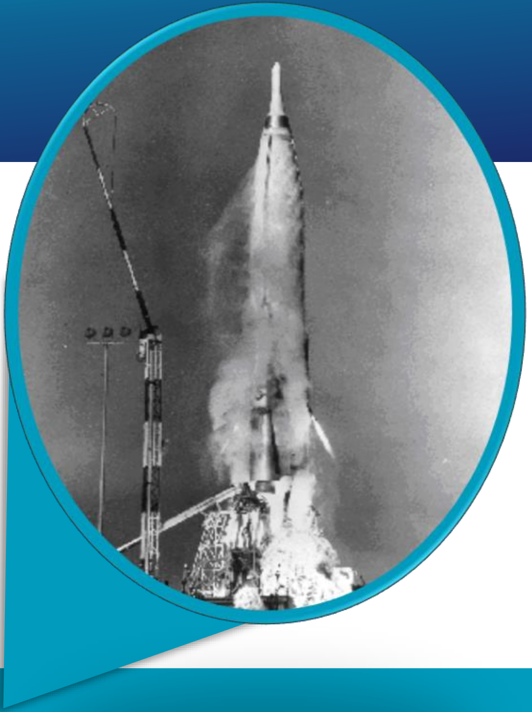


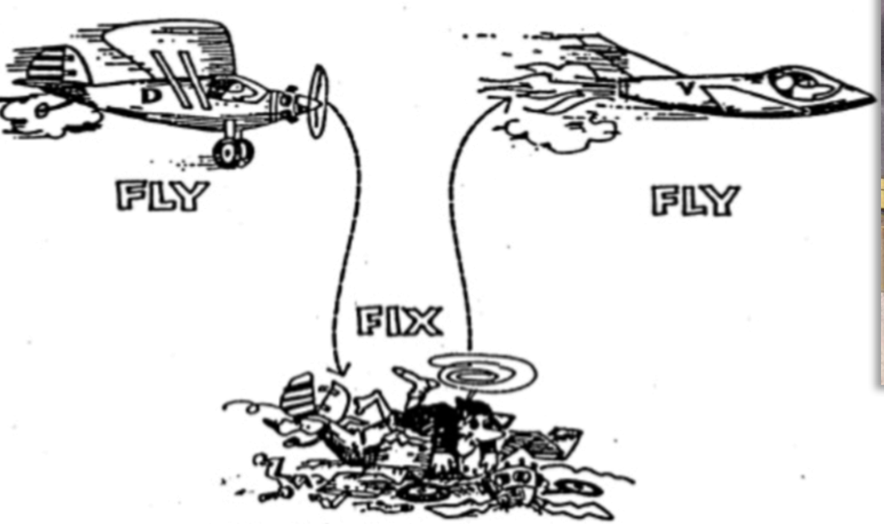


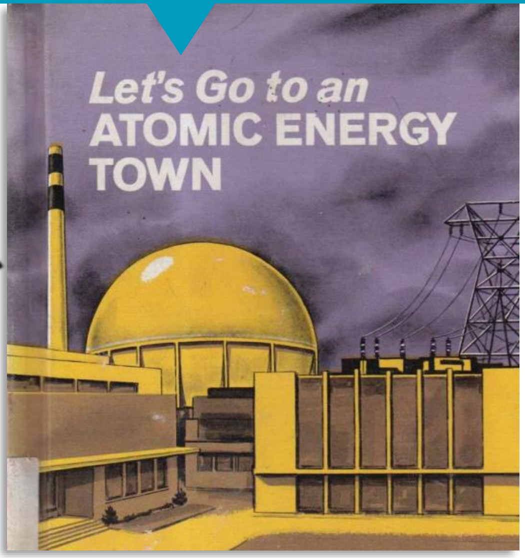


System Safety before System Safety

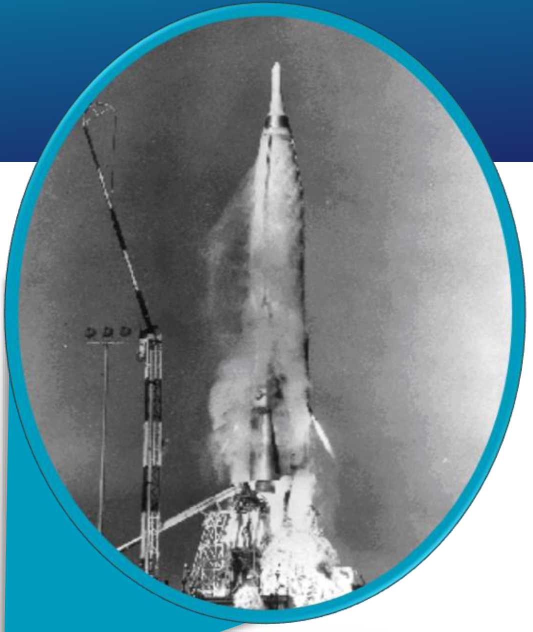




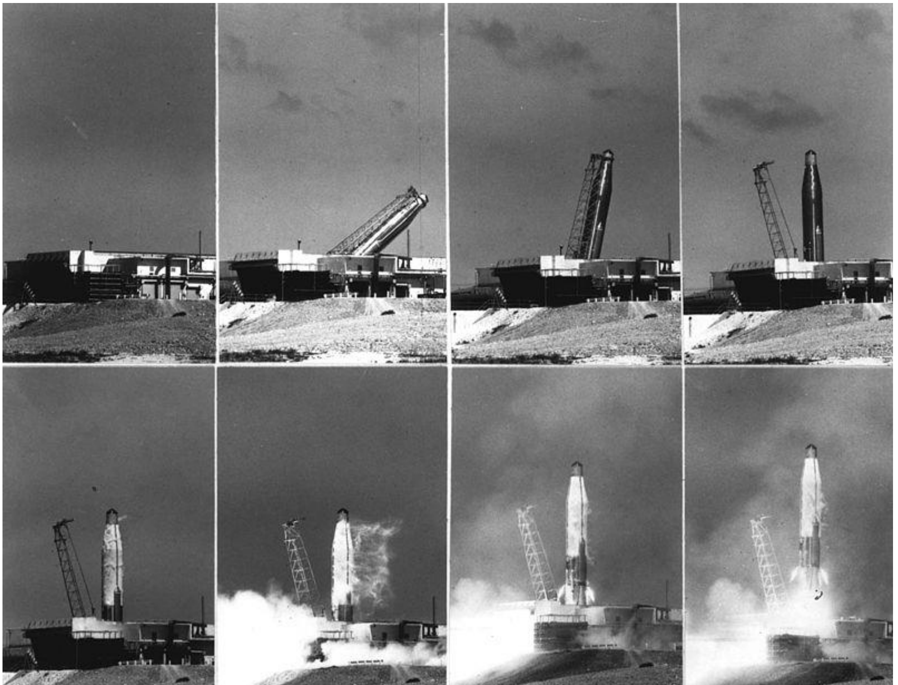




New Systems, New Problems



- Atlas and Titan intercontinental ballistic missiles
- Developed in the 50s
- Focus on the reliability of individual component or subsystem
- Lack of systematic assessment of system safety



- Interface problems went unnoticed until it was too late
- Four missile blew up in their silos during operational testing, within 18 months from becoming operational
- Extremely low launch success rate
- Losses investigation pointed to deficiencies in design, operations, and management

‘Organised Common Sense’


MIL-STD-882B
30 March 1984
SUPERSEDING
MIL-STD-882A
28 June 1977

MILITARY STANDARD

MIL-STD-882B SYSTEM SAFETY PROGRAM REQUIREMENTS

AMSC Number F3329 FSC SAFT

DISTRIBUTION STATEMENT A
Approved for Public Release - Distribution Unlimited

NOTICE 1

DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

System Safety Program Requirements
MIL-STD-882B

1. This Military Standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: HQ Air Force Systems Command (PLEQ ComSO), Andrews AFB, Washington, DC 20334-5000, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

- Only in 1960s system safety began to take on its own role

- Born to understand and manage the ‘new complexity’ of engineering systems

- The Minuteman ICBM became the first (weapon) system to have a contractual, formal, disciplined system safety program

- The space program was the second major area to apply system safety approaches in a disciplined way

- **Search for tools able to deal with systems as a whole rather than with subsystems or components → the complexity of new systems (and the weakness of judgement tools) lies with their interconnected nature**


WEATHER

The Arizona Daily Star

★ An Independent NEWSpaper Printing The News Impartially ★

TUCSON, ARIZONA, SATURDAY MORNING, JANUARY 28, 1967

FINAL

TEN CENTS

THIRTY PAGES

Apollo Training Craft Explodes

ASTRONAUTS DIE IN FIERY CAPSULE

VIRGIL I. GRISSOM ... Veteran command pilot

EDWARD H. WHITE II ... Spacewalk hero

ROGER B. CHAFFEE ... Rookie astronaut

U.S. Signs Outer Space N-Treaty

'Inspiring Moment'

3 Spacemen Trained In Arizona

Three-Man Crew Killed Instantly

New Problems, New Solutions

Hazard-focused

Failure mode and effects analysis
(FMEA, 50s)

Preliminary Hazard List
(PHL, 60s)

Hazard and Operability Study
(HAZOP, 60s)

Management Oversight and Risk Tree
(MORT, 1972)

System-focused

Reliability Block Diagrams
(RBDs, 60s)

Fault Trees
(FTs, 1962)

Event Trees
(FTs, 1974)

New Problems, New Solutions

Hazard-focused

Failure mode and effects analysis
(FMEA, 50s)

Preliminary Hazard List
(PHL, 60s)

Hazard and Operability Study
(HAZOP, 60s)

Management Oversight and Risk Tree
(MORT, 1972)

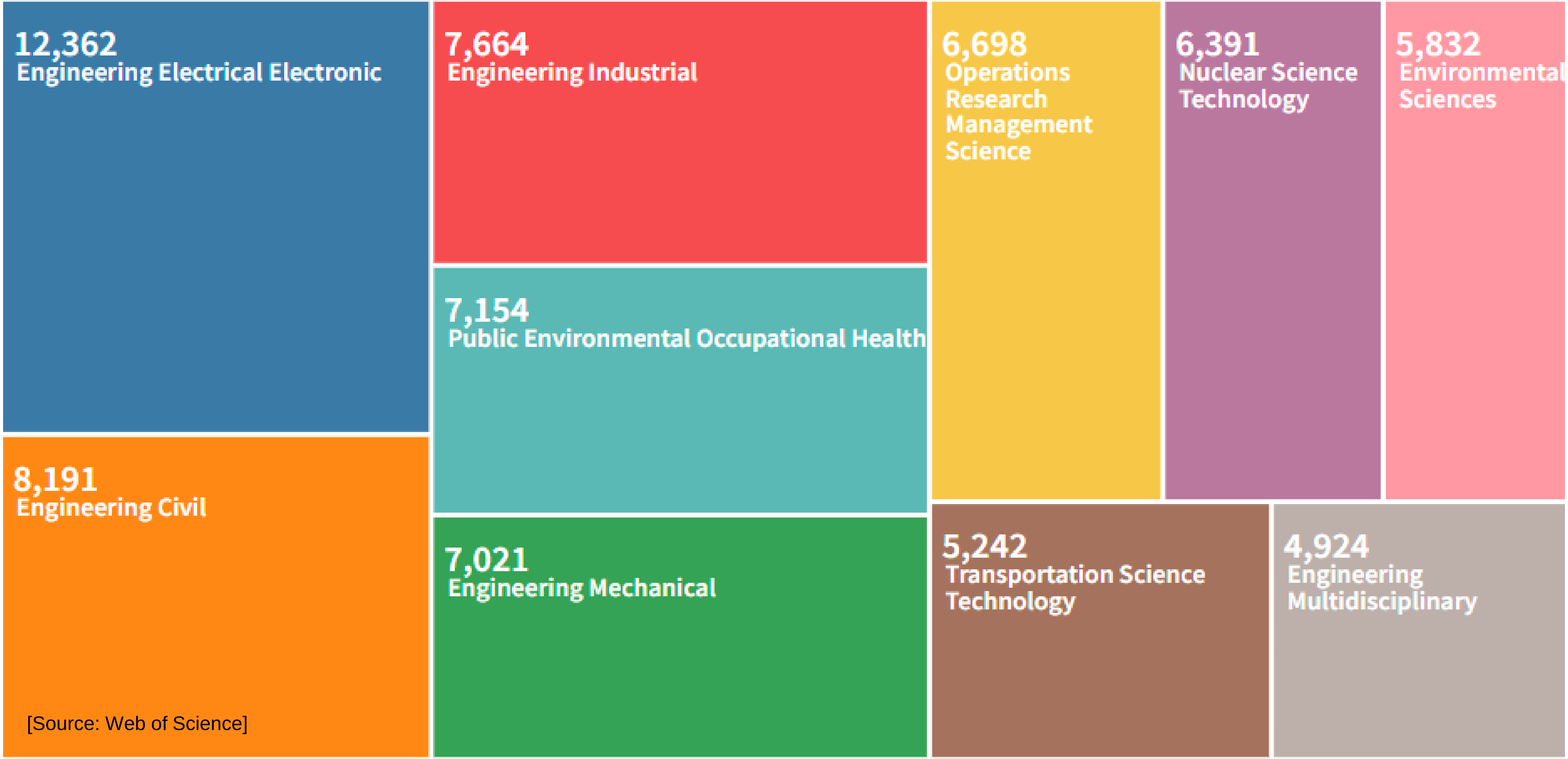
System-focused

Reliability Block Diagrams
(RBDs, 60s)

Fault Trees
(FTs, 1962)

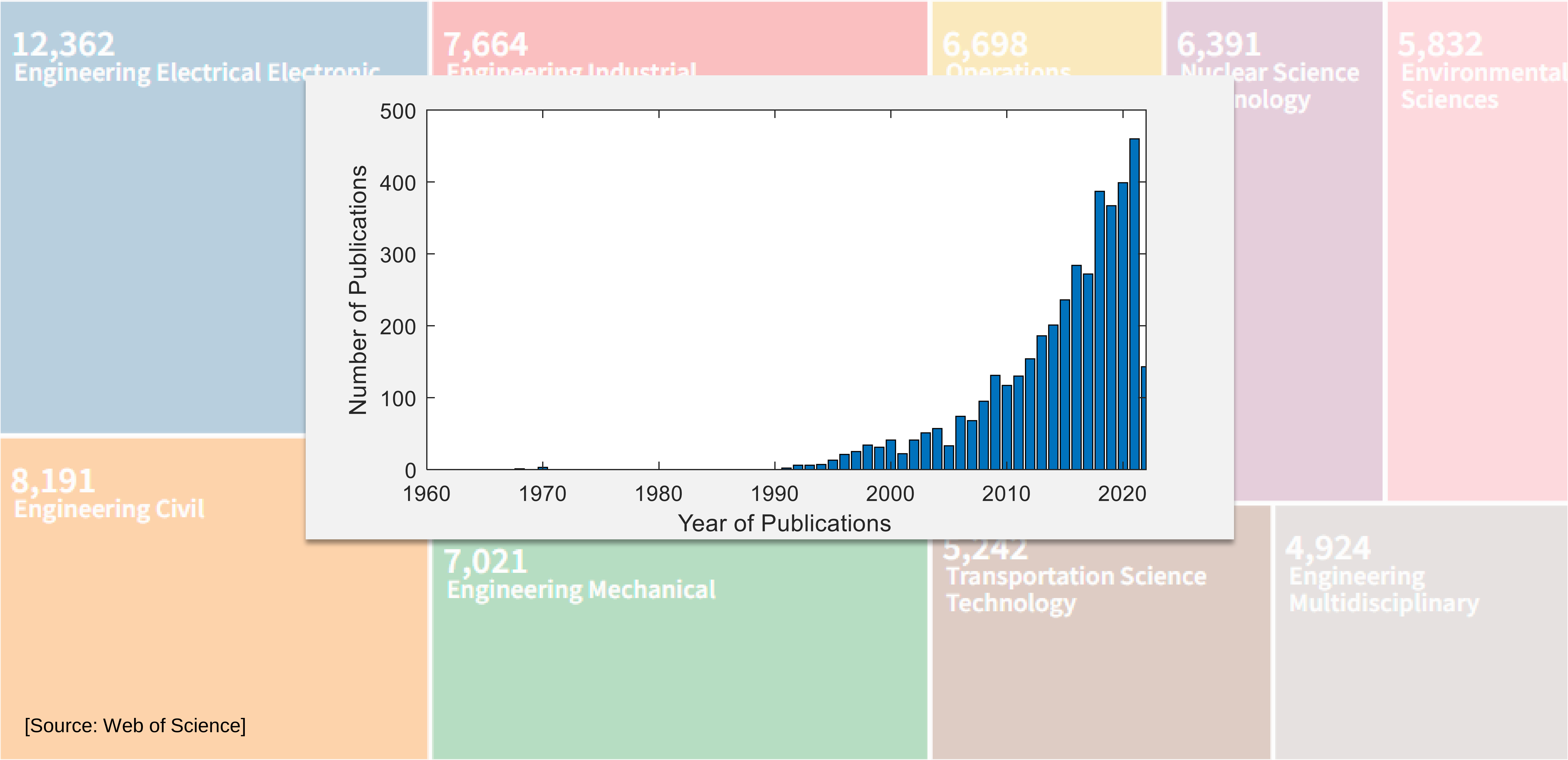
Event Trees
(FTs, 1974)

Where are we at?



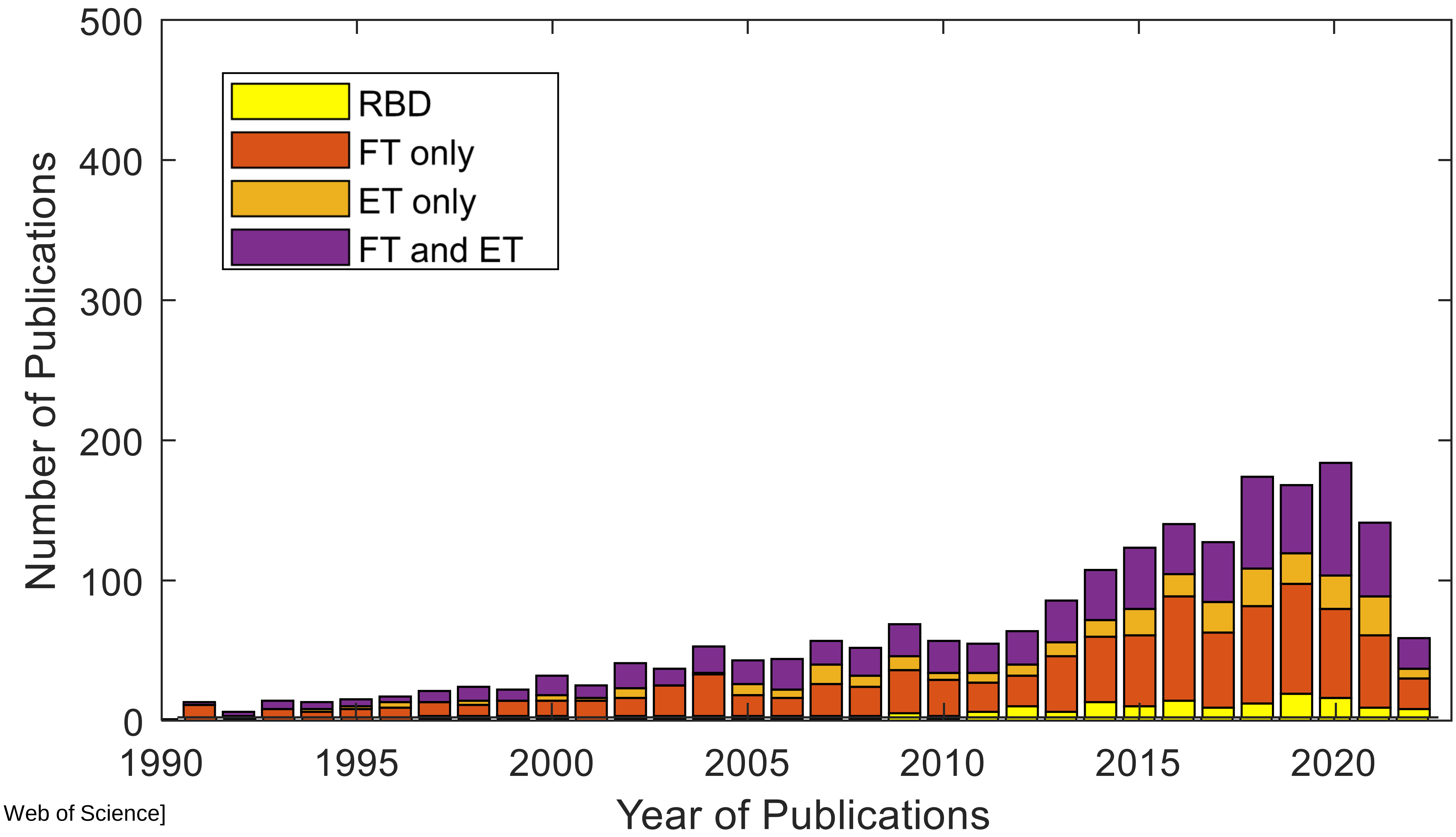
[Source: Web of Science]

Where are we at?



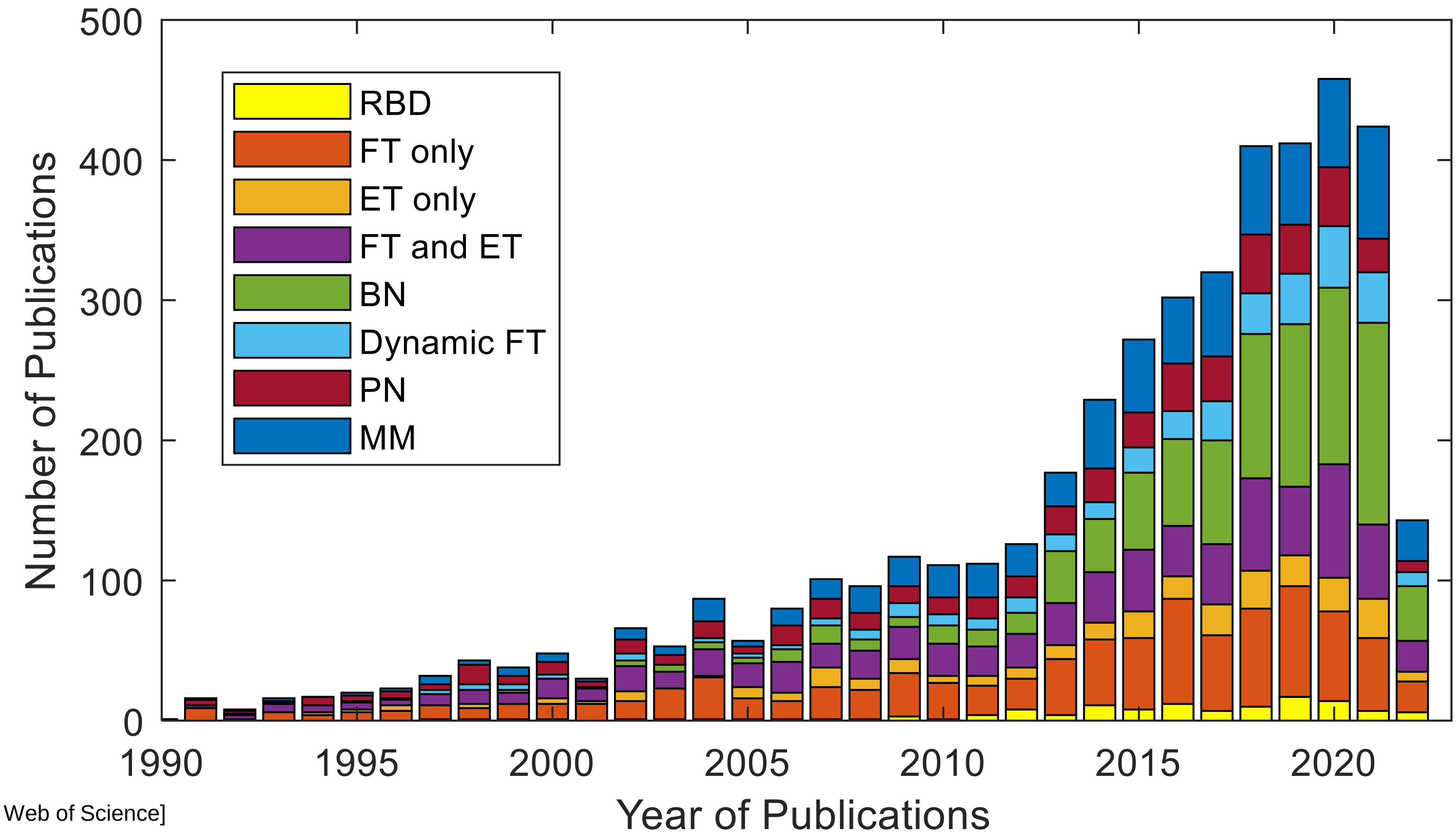
[Source: Web of Science]

Where are we at?



[Source: Web of Science]

Where are we at?

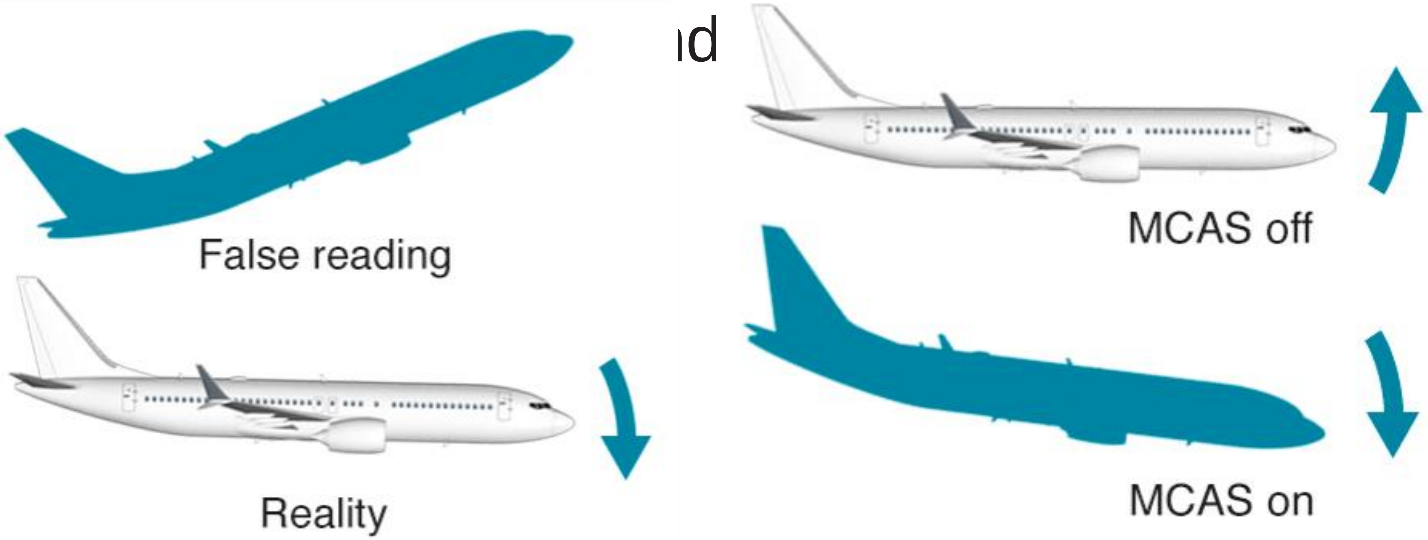


[Source: Web of Science]

New Systems, New Problems…again?

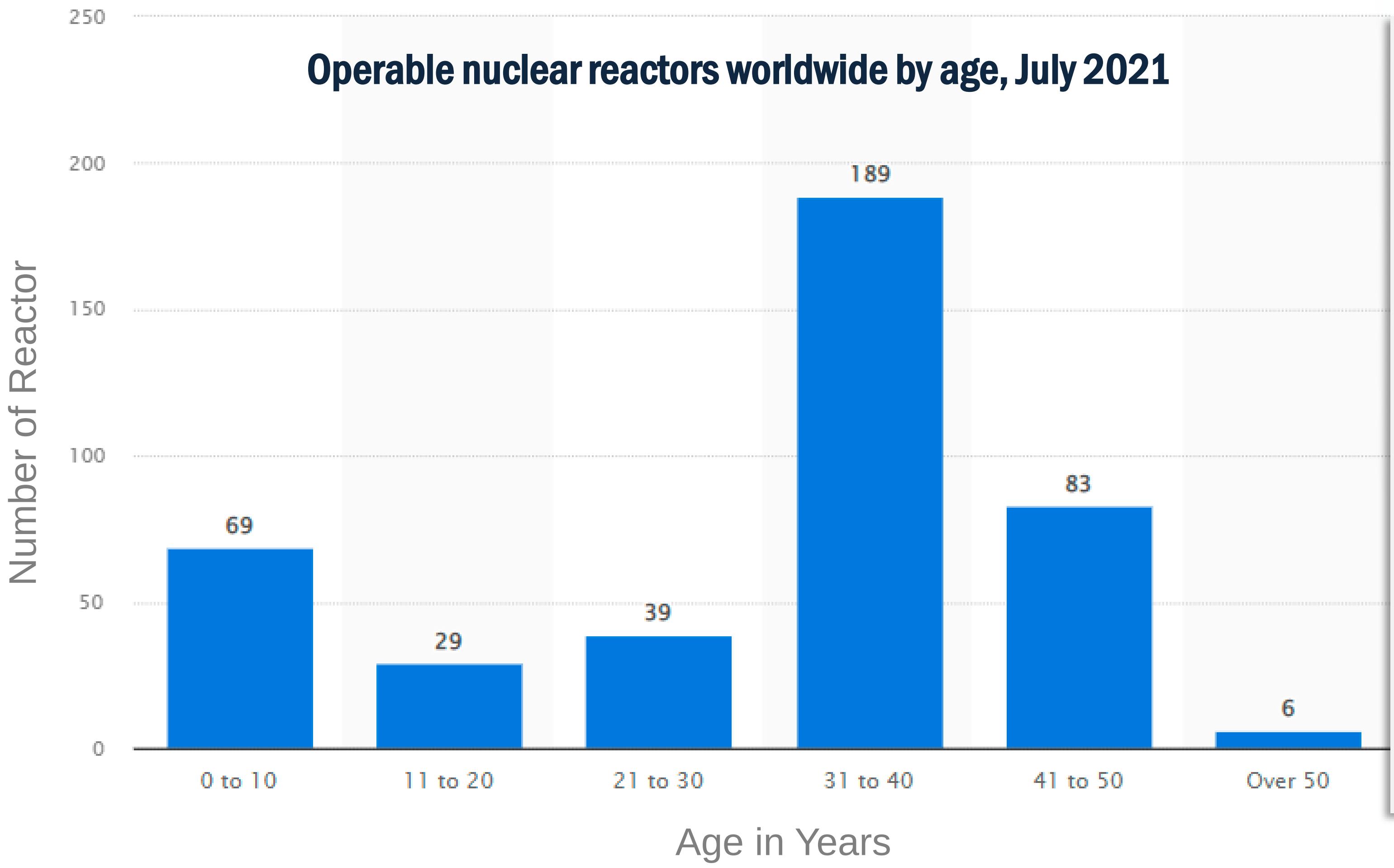
BOEING 737 max:

- Manoeuvring Characteristics Augmentation System (MCAS)
- Safety-analysis led by Boeing concluded there would be little risk in the event of an MCAS failure
- Assumed pilots response time to an unexpected MCAS
ıd



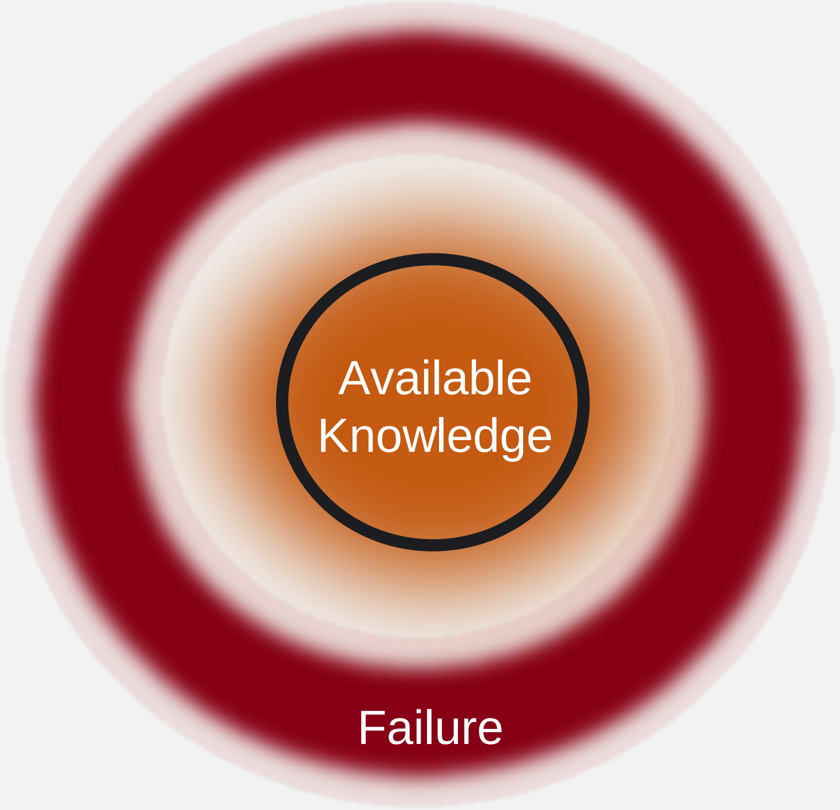
Old Systems, New Problems

“The nuclear community is facing new challenges as commercial nuclear power plants get older”
[IAEA,1990]



- More than 2/3 of the 415 reactors in operation are over 30 years old
- Around 40 years operational lifetime
- Around 100 reactors already granted life extension licenses
- Ageing may increase the risk of loss or reduction of functional capability of key plant components
- Impairment of one or more multiple levels of protection afforded by defence in depth

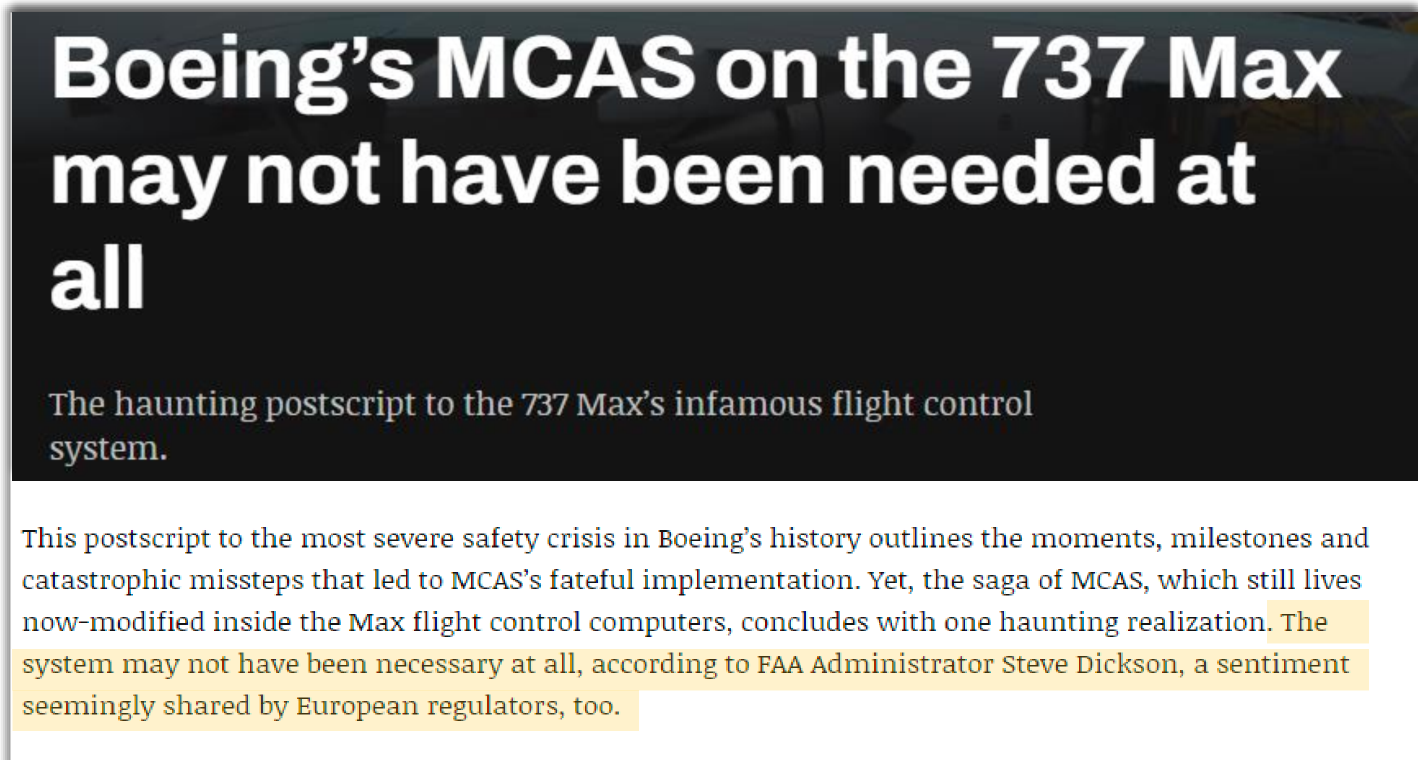
…and just Old Problems



- Conservative Approach
- Strong Assumptions
- **Unknown level of conservatism**

"In the absence of methods that explicitly account for uncertainties, seeking reasonable conservatism in nuclear safety analyses can quickly lead to extreme conservatism. The rate of divergence to extreme conservatism is often beyond the expert analysts' intuitive feeling"

[K.Jamaly, Achieving reasonable conservatism in nuclear safety analyses,
RESS, Volume 137, May 2015, Pages 112-119]



Boeing's MCAS on the 737 Max may not have been needed at all

The haunting postscript to the 737 Max's infamous flight control system.

This postscript to the most severe safety crisis in Boeing's history outlines the moments, milestones and catastrophic missteps that led to MCAS's fateful implementation. Yet, the saga of MCAS, which still lives now-modified inside the Max flight control computers, concludes with one haunting realization. The system may not have been necessary at all, according to FAA Administrator Steve Dickson, a sentiment seemingly shared by European regulators, too.

University of Nottingham
UK | CHINA | MALAYSIA

Current Challenges

- High level of automation and control technology
  → systems are un-negligibly dynamic → **Lack of dependency modelling**
  → human-technology interface → **No depiction of dynamic features**
  → maintenance strategies are increasingly complex → **Limited maintenance models**
- Life extension
  → system behaviour changes along its life-cycle → **Constant rates assumption**
- Uncertainty and Modelling
  → conservatism comes at a cost → **Modelling limitations balanced by conservative assumptions**

TRADITIONAL METHODOLOGIES

- Lack of dependency modelling
- No depiction of dynamic features
- Limited maintenance models
- Constant rates assumption
- Modelling limitations balanced by conservative assumptions

Current Challenges

- High level of automation and control technology

  → systems are un-negligibly dynamic

  → human-technology interface

  → maintenance strategies are increasingly complex

- Life extension

  → system behaviour changes along its life-cycle

- Uncertainty and Modelling

  → conservatism comes at a cost

SIMULATION-BASED SOLUTIONS

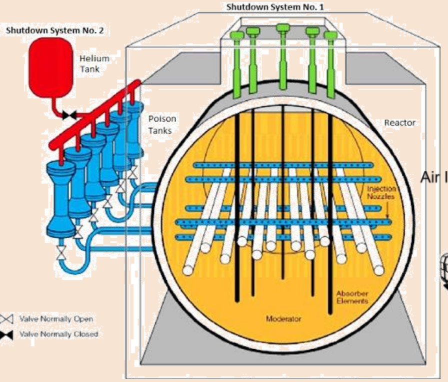
Computationally unfeasible for large-scale systems

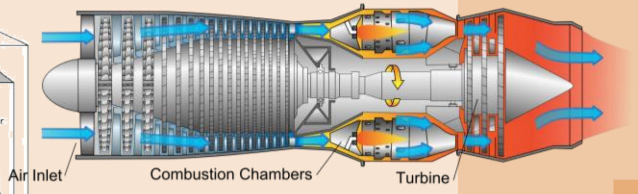
What can we do differently?

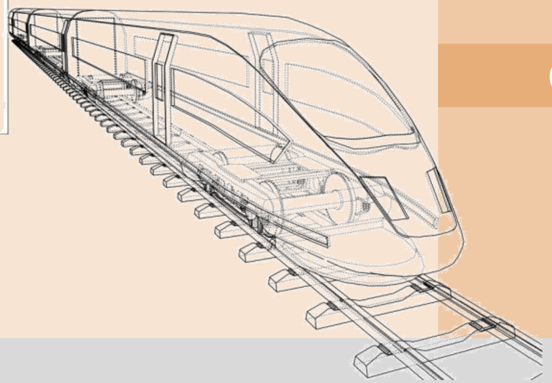
Methodology Overview

An Umbrella Methodology

FAMILIAR MODELLING LANGUAGE







REALISTIC RISK MODELLING

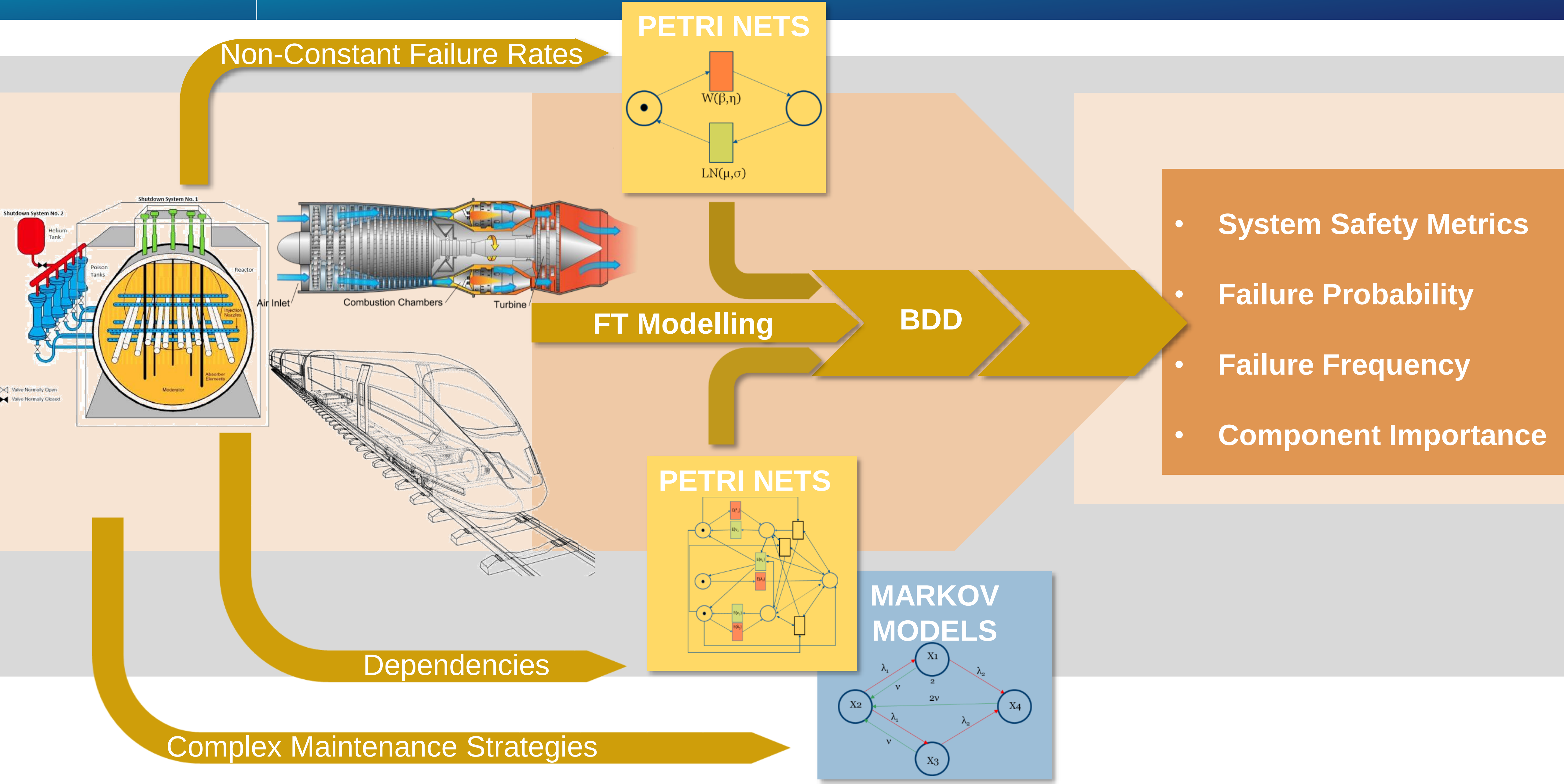
- Dependencies
- Non-Constant Failure Rates
- Complex Maintenance Strategies

ANALYSIS ACCURACY

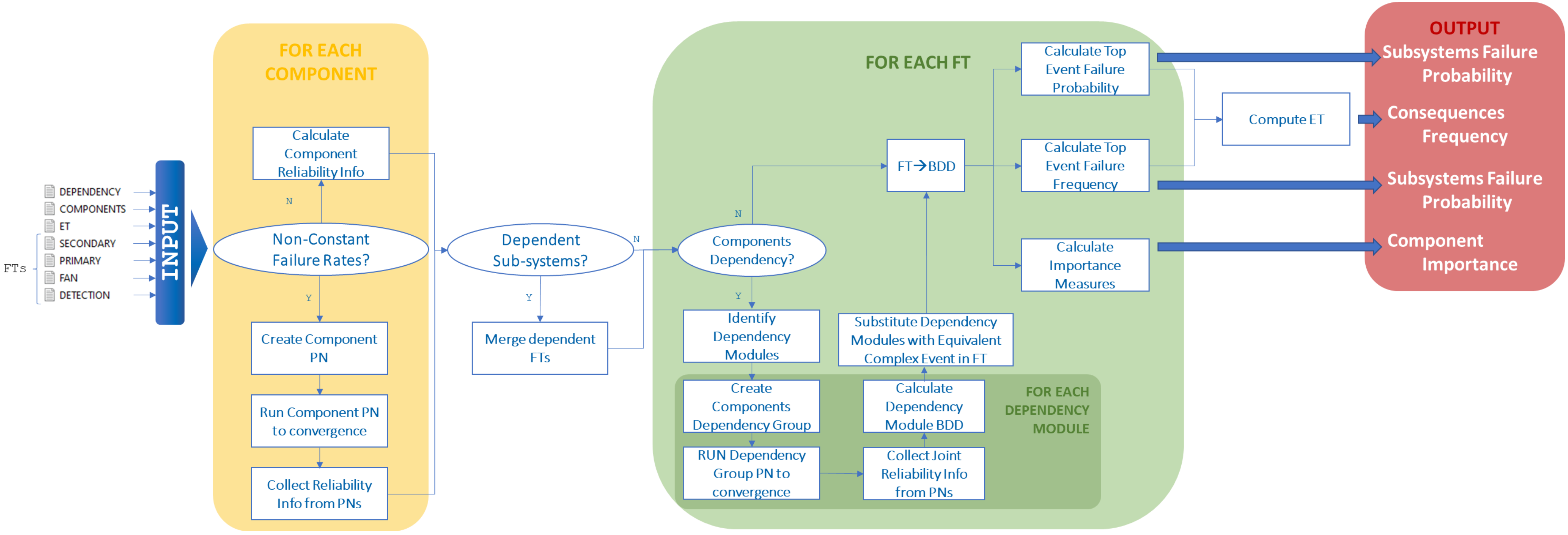
- **System Safety Metrics**
- **Failure Probability**
- **Failure Frequency**
- **Component Importance**

COMPUTATIONAL FEASIBILITY

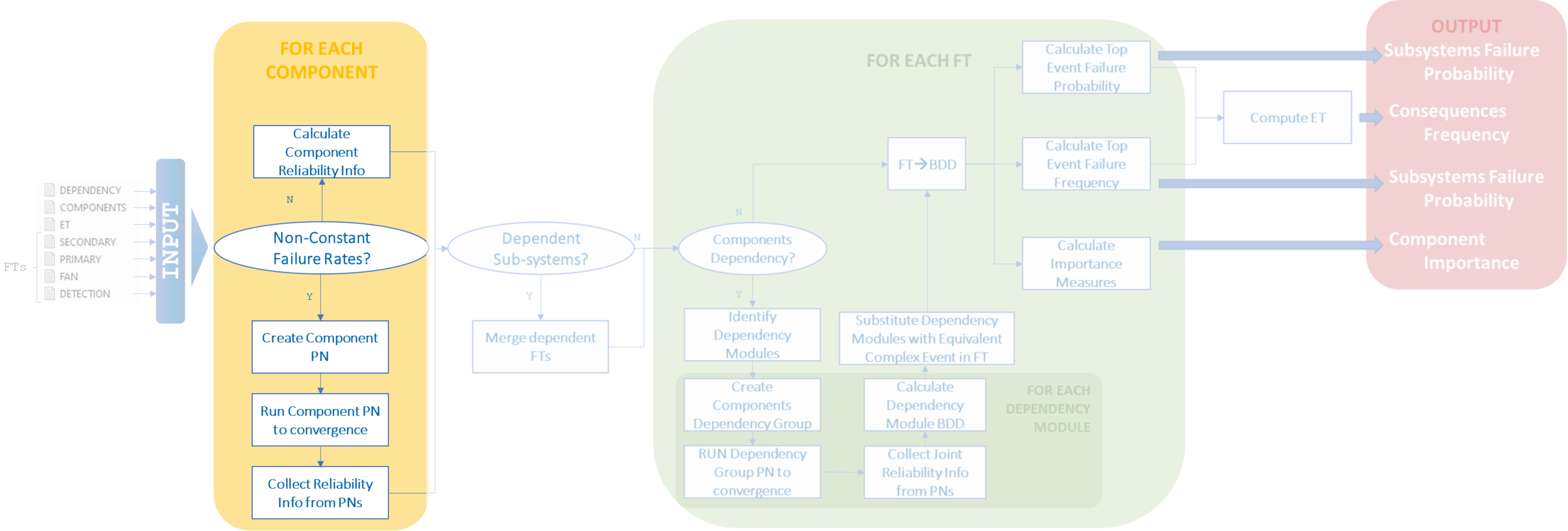
An Umbrella Methodology



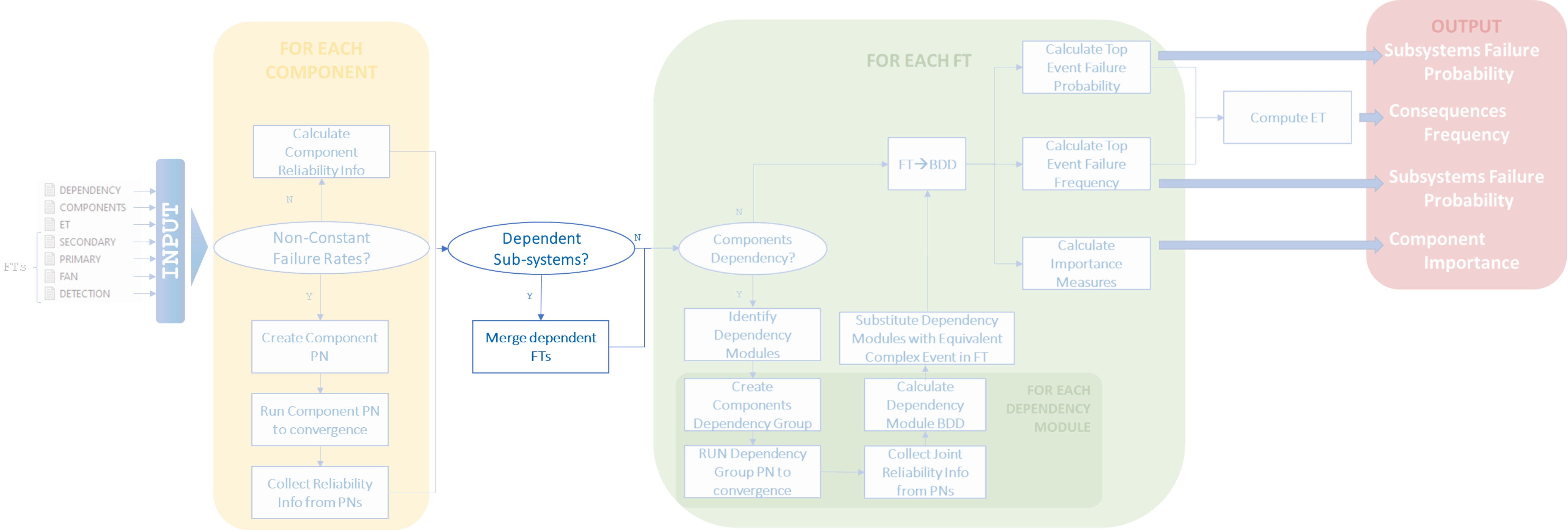
Step by Step


FTs
DEPENDENCY
COMPONENTS
ET
SECONDARY
PRIMARY
FAN
DETECTION
INPUT
FOR EACH COMPONENT
Calculate Component Reliability Info
N
Non-Constant Failure Rates?
Y
Create Component PN
Run Component PN to convergence
Collect Reliability Info from PNs
Dependent Sub-systems?
N
Y
Merge dependent FTs
FOR EACH FT
Components Dependency?
N
Y
FT→BDD
Identify Dependency Modules
Substitute Dependency Modules with Equivalent Complex Event in FT
Create Components Dependency Group
Calculate Dependency Module BDD
RUN Dependency Group PN to convergence
Collect Joint Reliability Info from PNs
FOR EACH DEPENDENCY MODULE
Calculate Top Event Failure Probability
Calculate Top Event Failure Frequency
Calculate Importance Measures
Compute ET
OUTPUT
Subsystems Failure Probability
Consequences Frequency
Subsystems Failure Probability
Component Importance

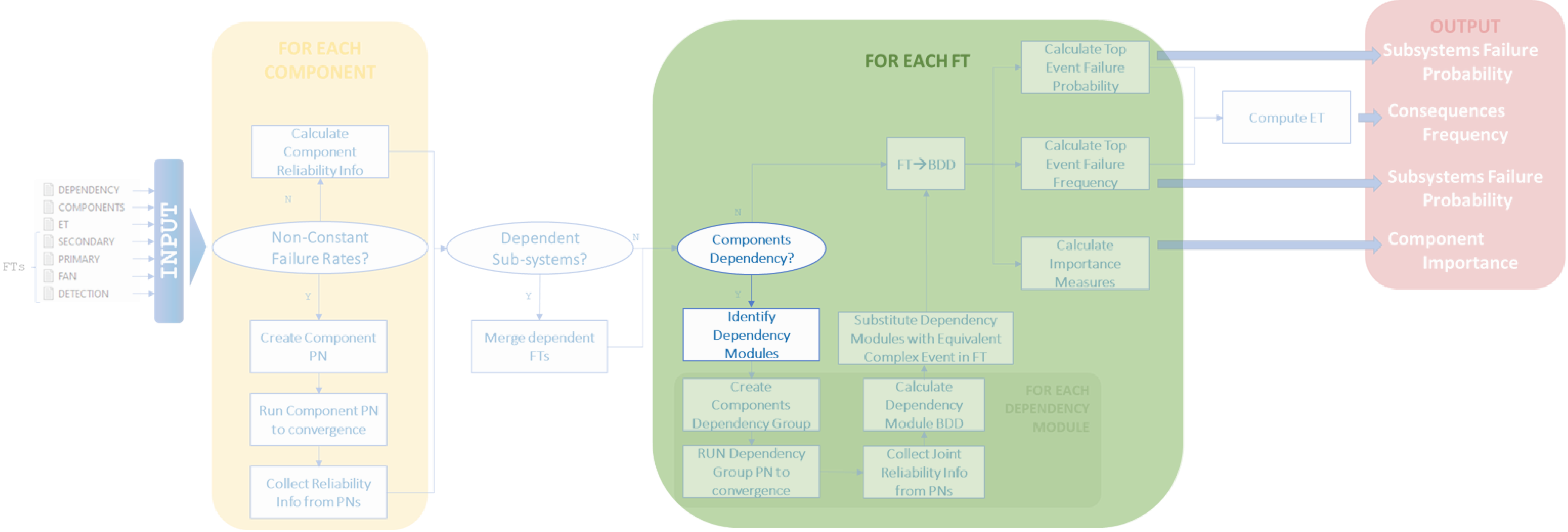
Step1: Component Reliability



Step 2: Independent FTs definition

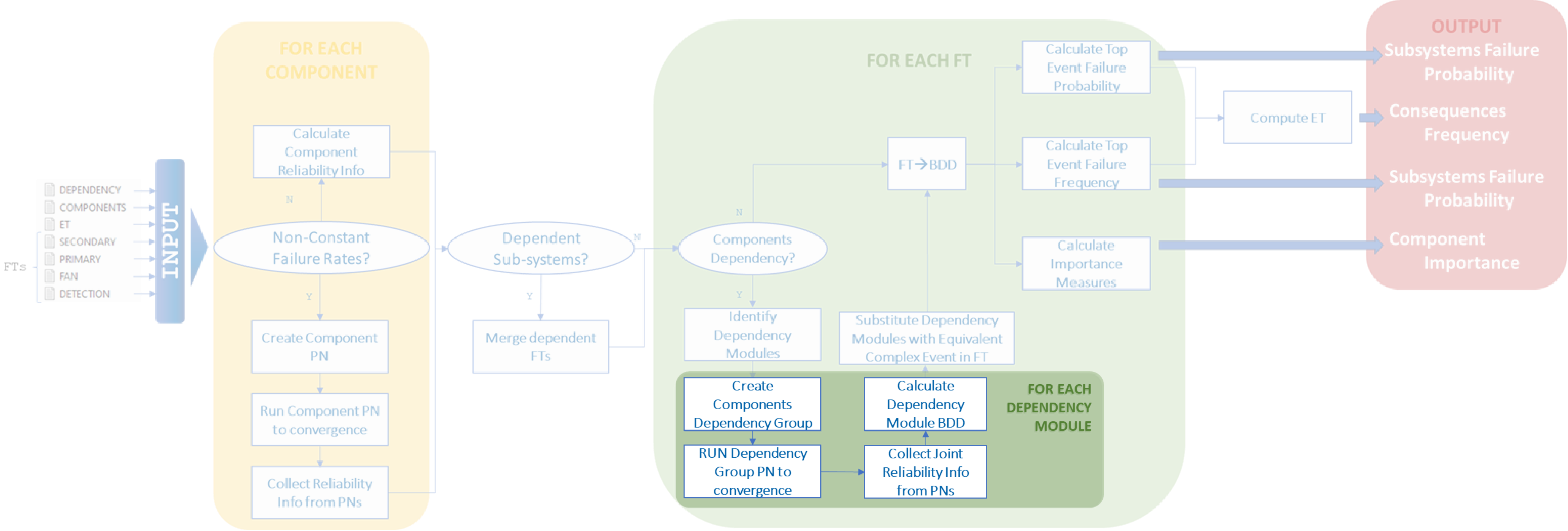


Step 3: Dependency Modules Identification

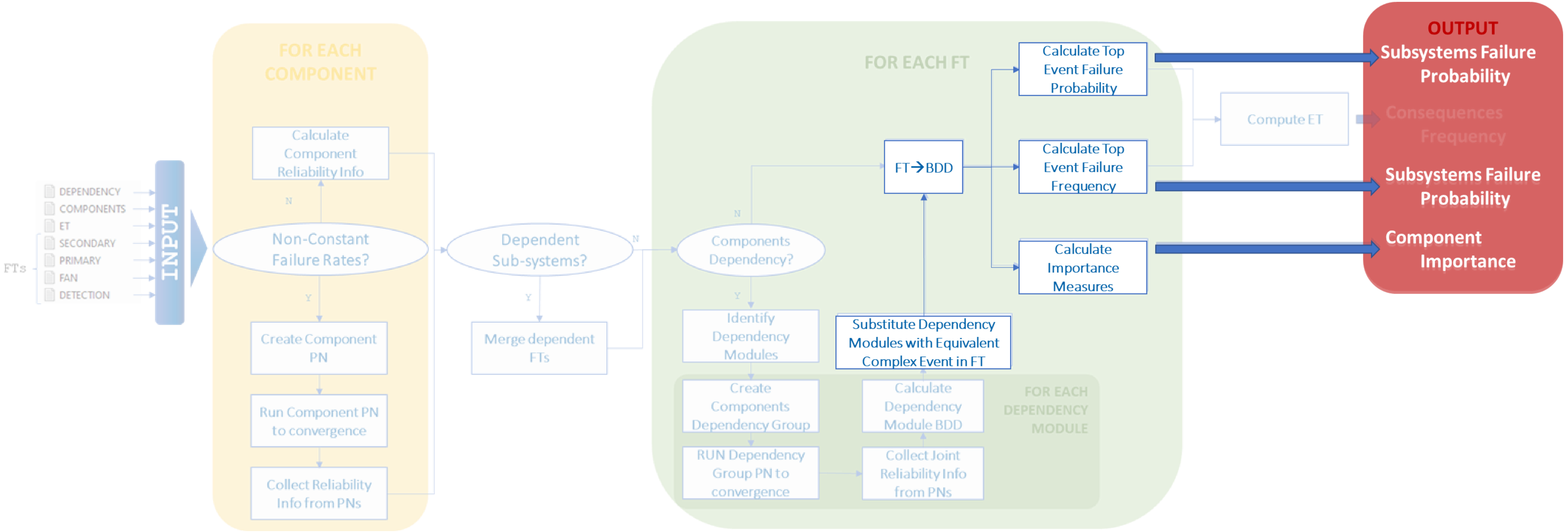


Dependency Modules → the smallest independent section of a FT model enclosing components dependent from each other

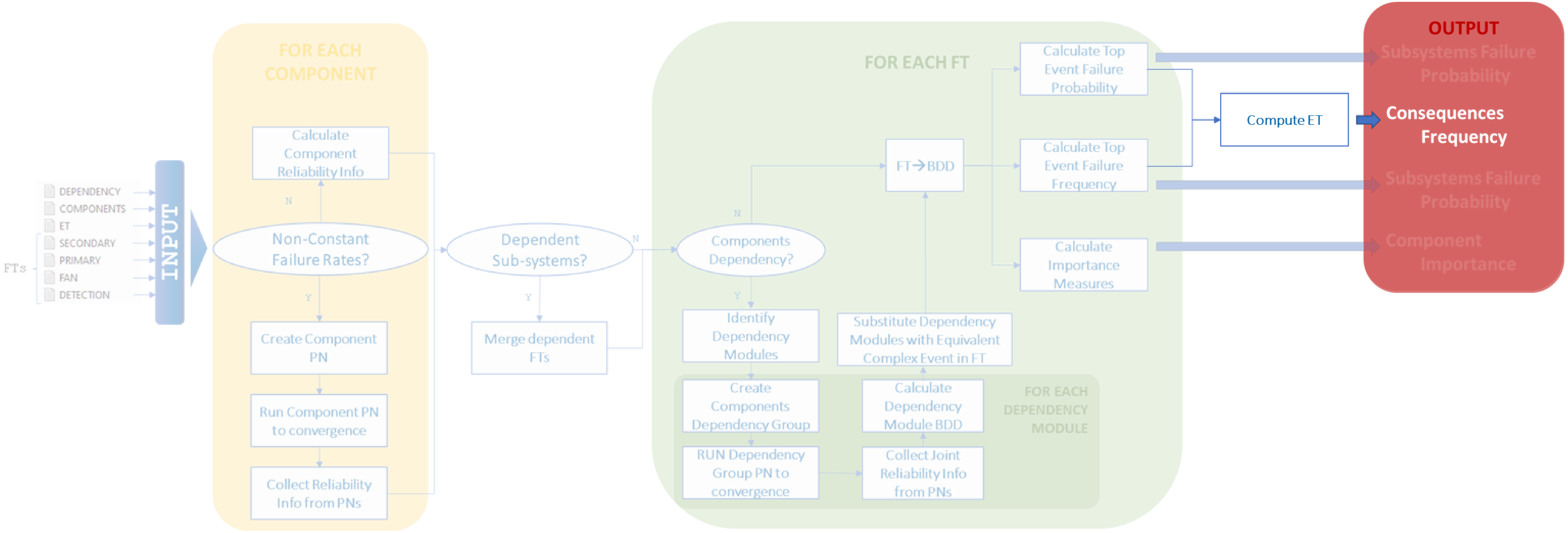
Step 4: Dependency Modules Computation



Step 5: FTs Computation



Step 6: ET computation



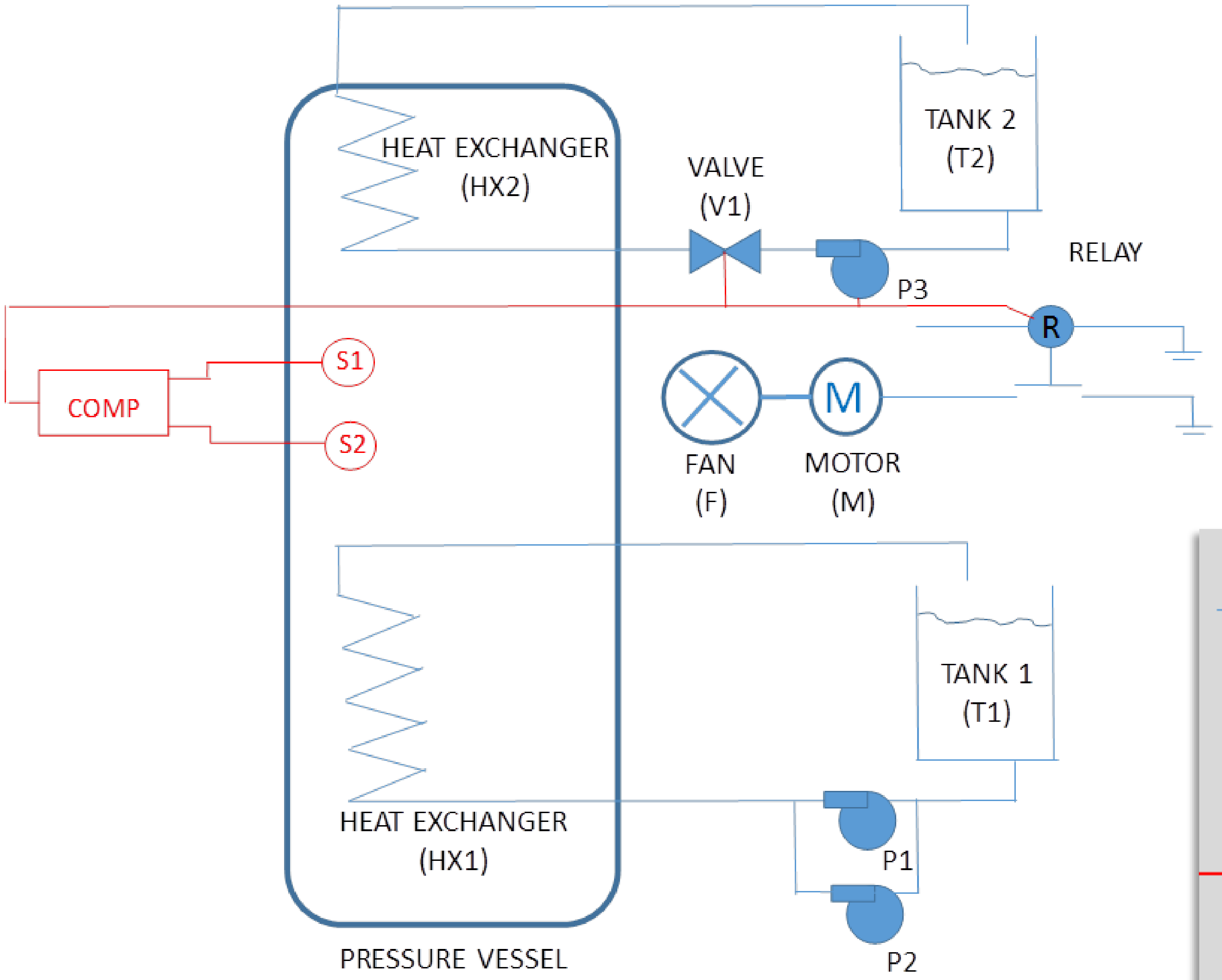
Hands On

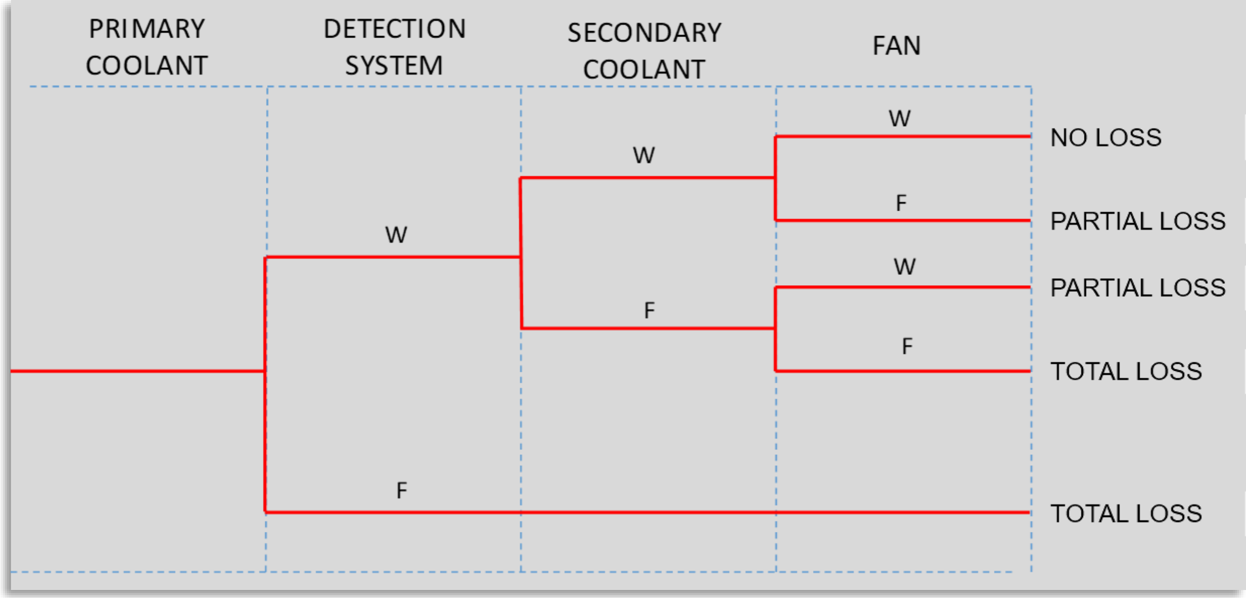
A simple case-study

Case-study

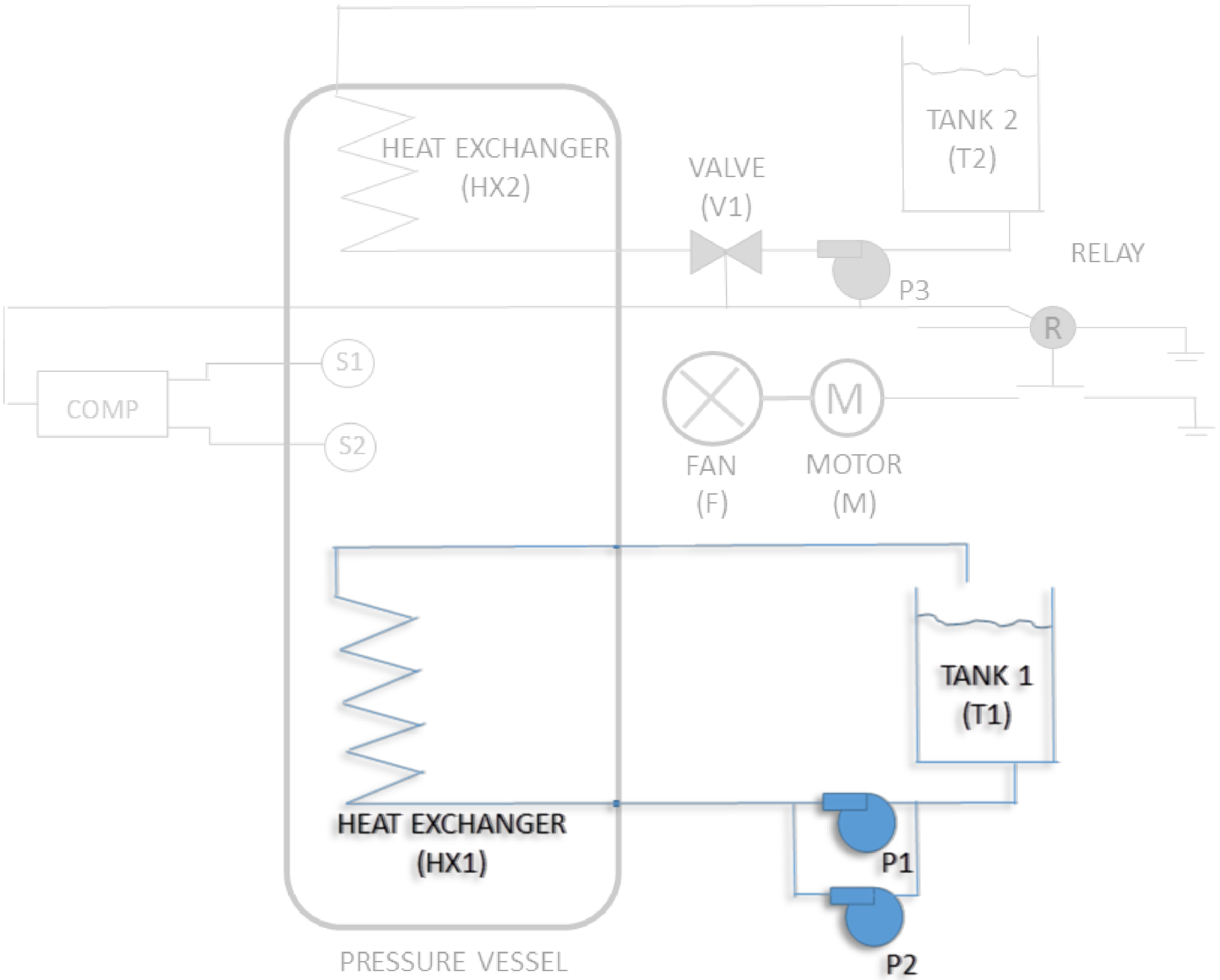
Overview:

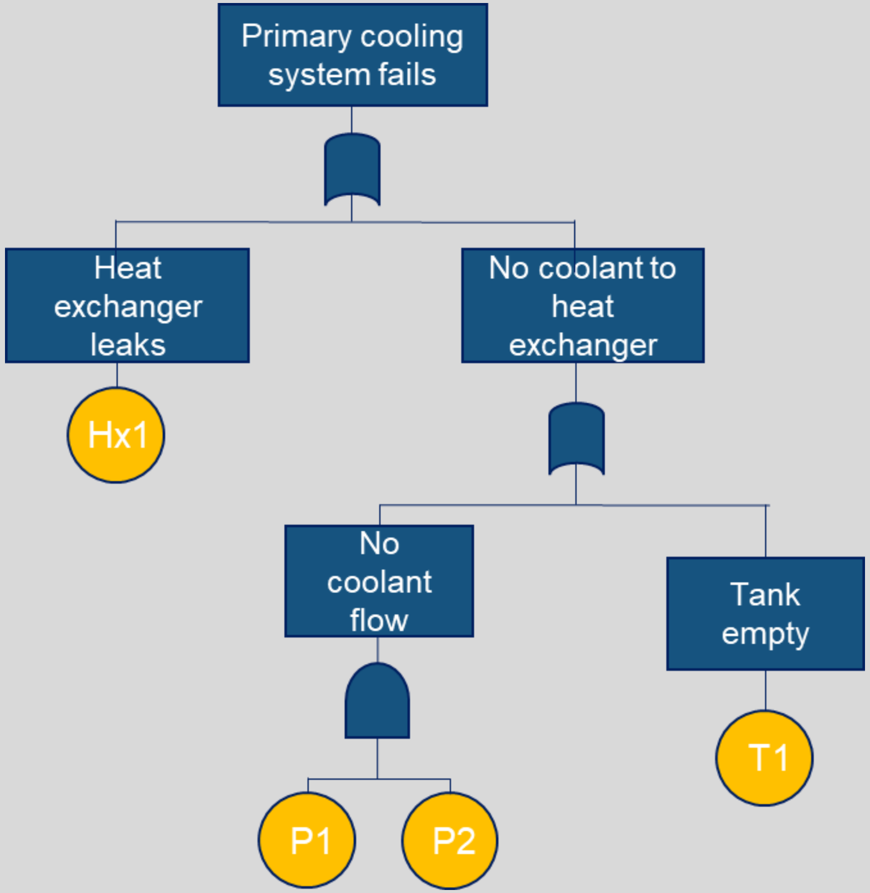
- Industrial cooling system
- 20y life cycle
- Complex features:
  - Aging Components
  - Complex Maintenance Strategies
  - Component Dependencies





Primary Cooling



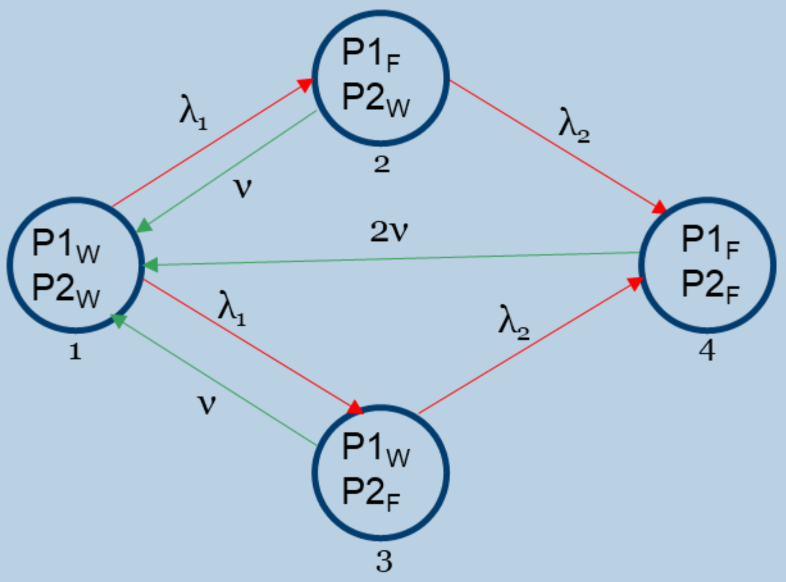


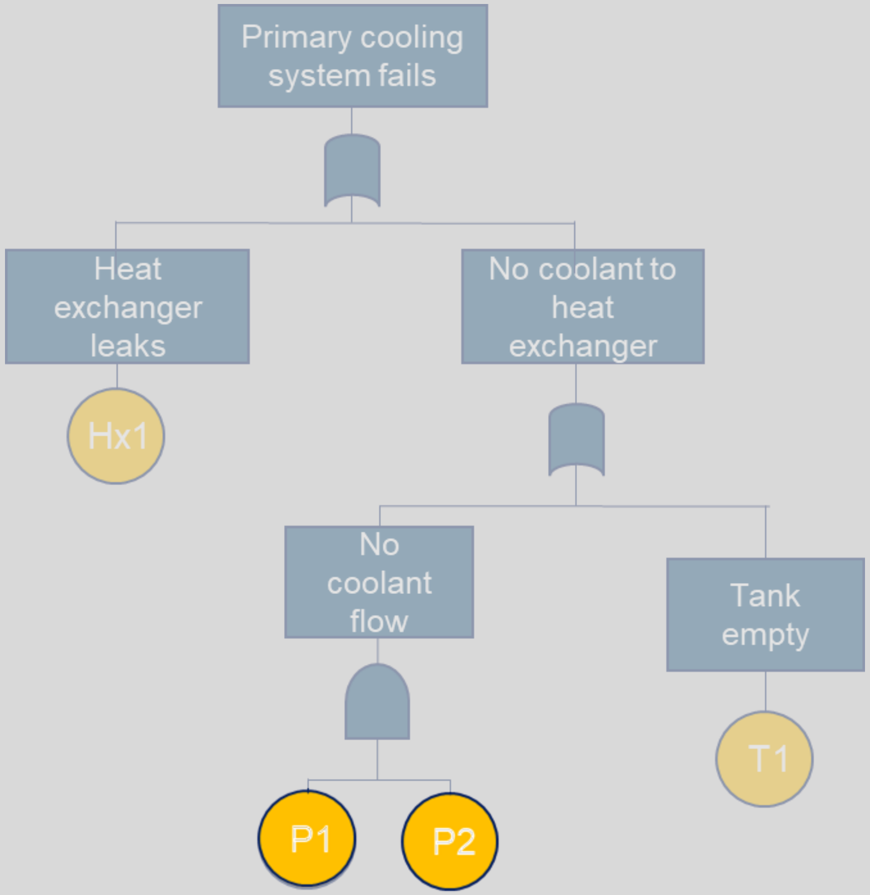
Primary Cooling

P1&P2 Dependency

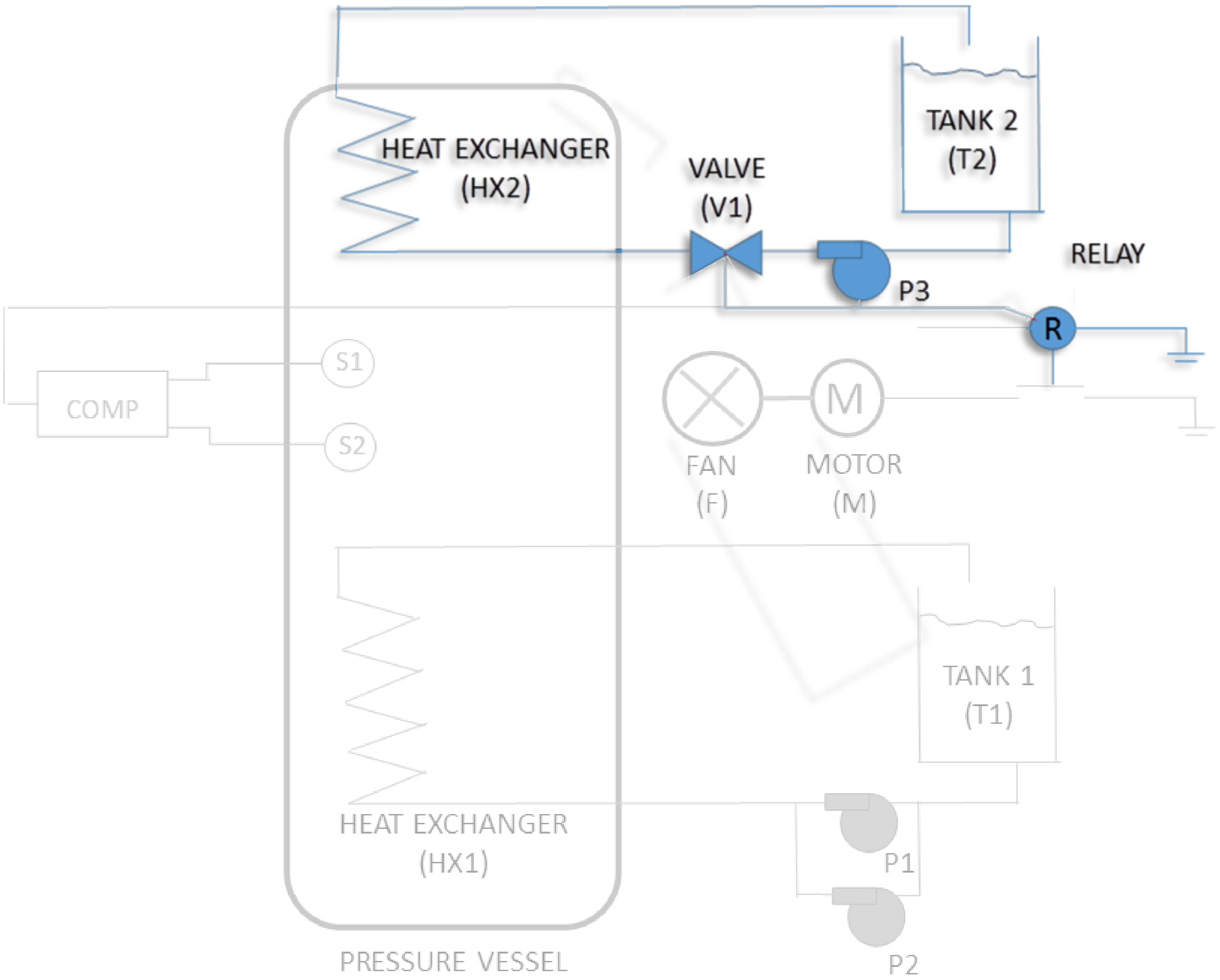
Failure of P1 (P2) increases load and failure rate of P2 (P1)

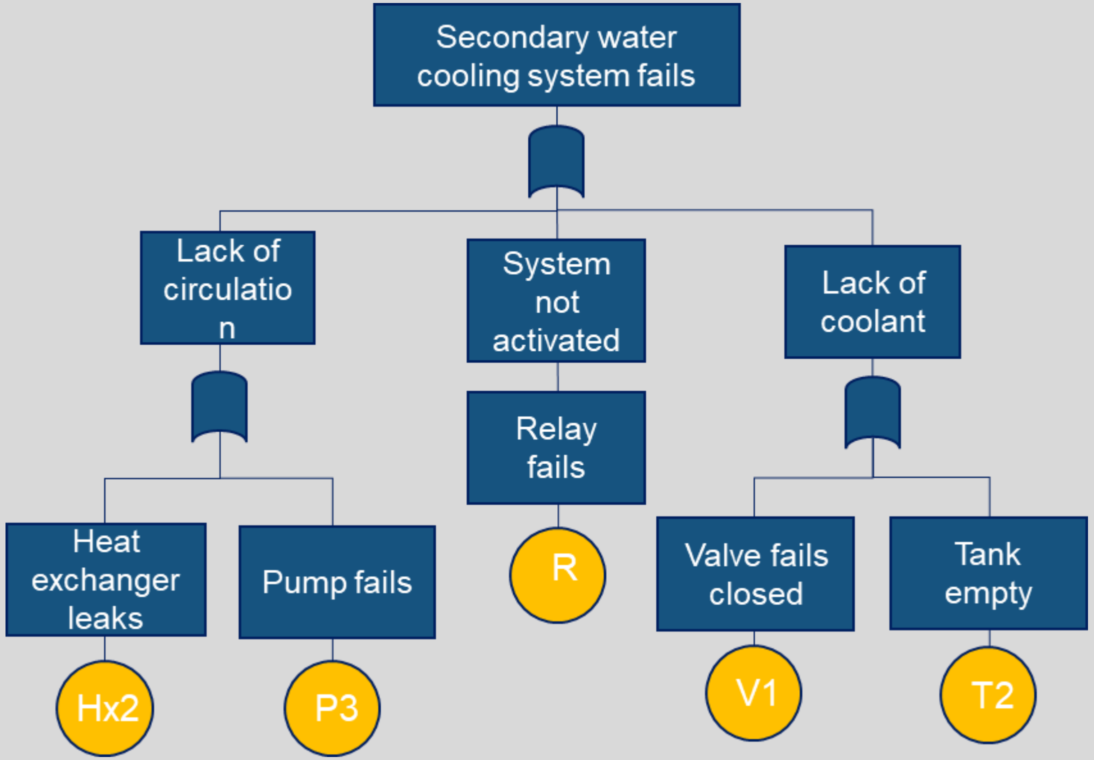
MARKOV MODEL





Secondary Water Cooling

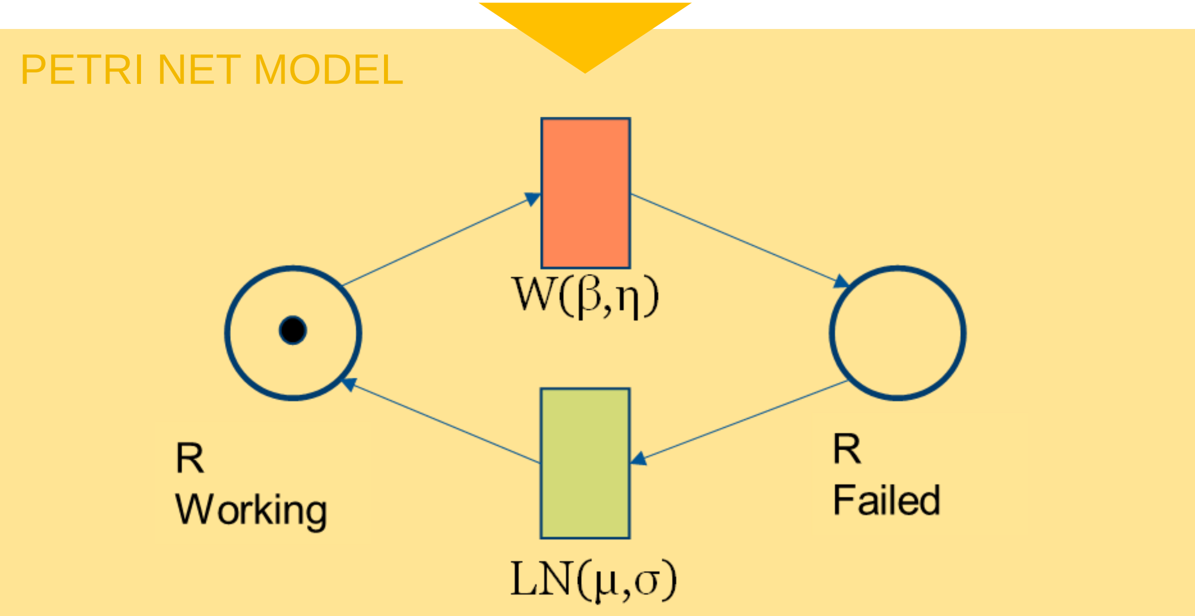


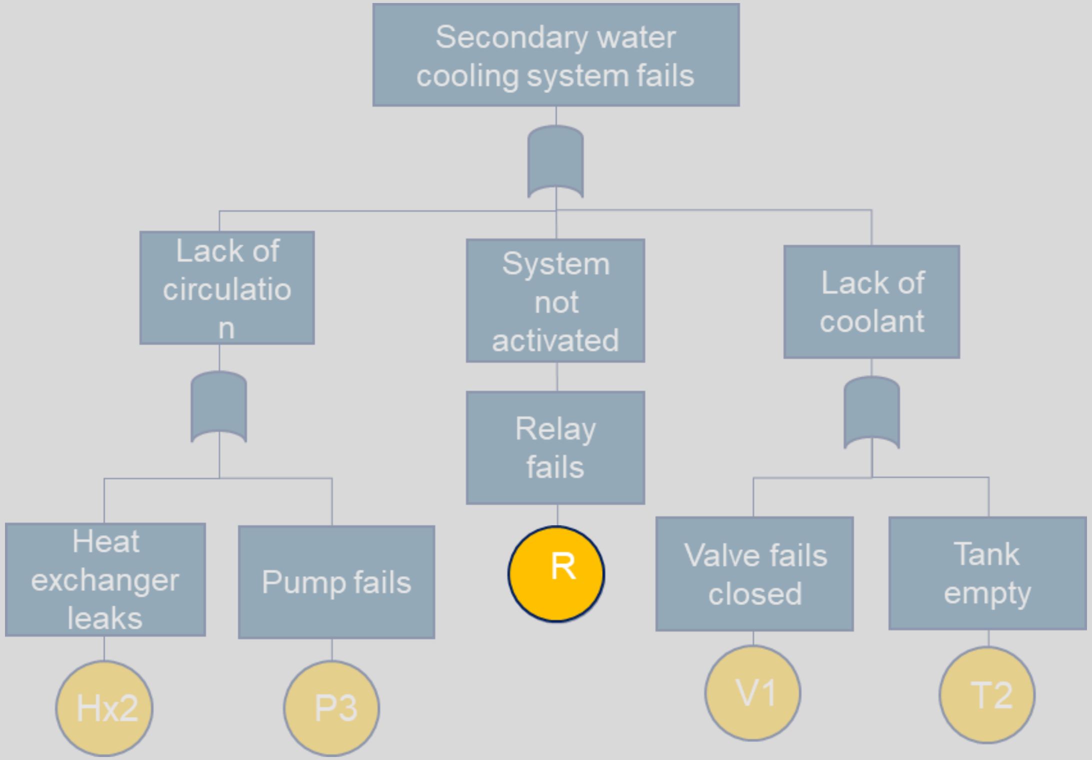


Secondary Water Cooling

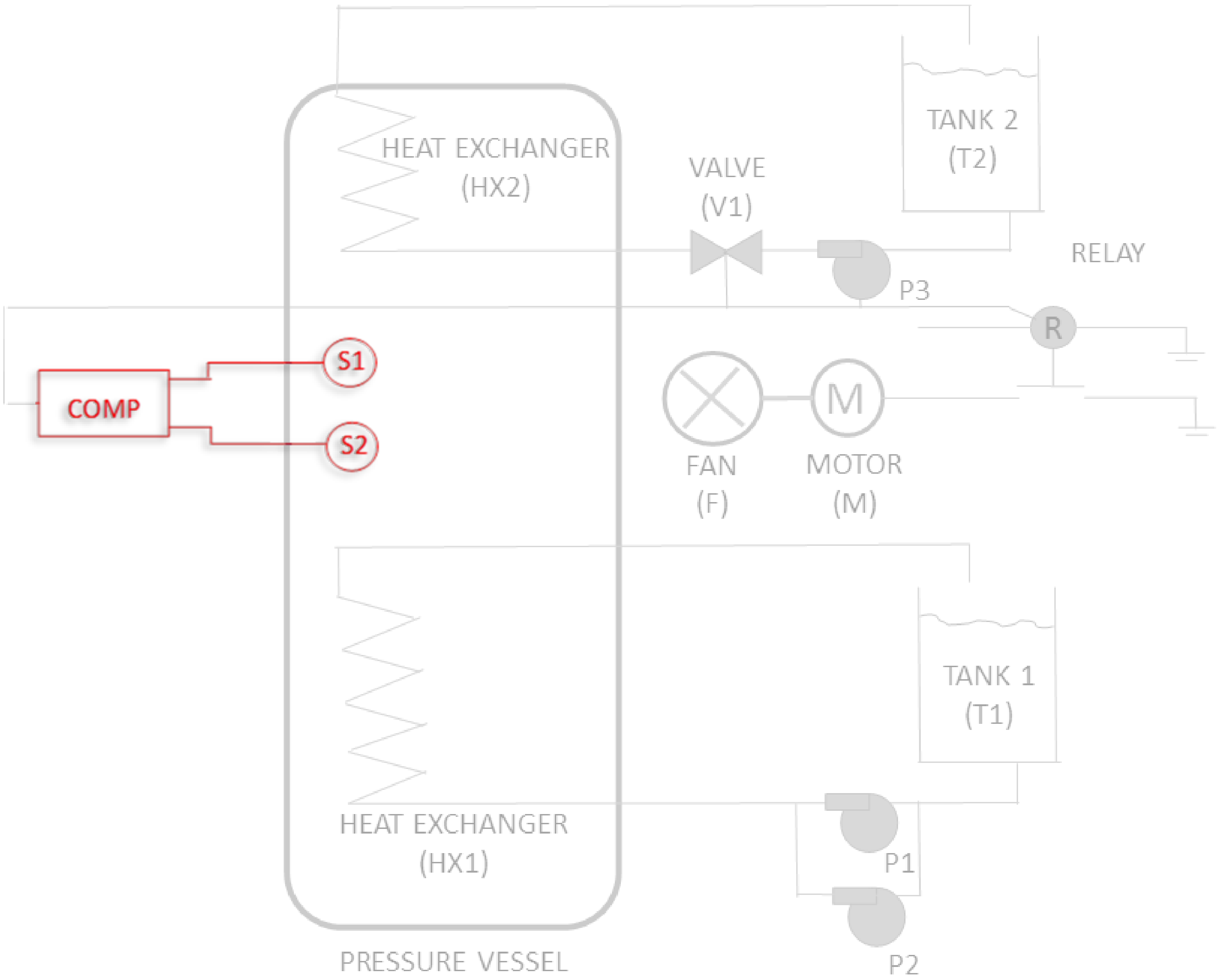
R Aging Component

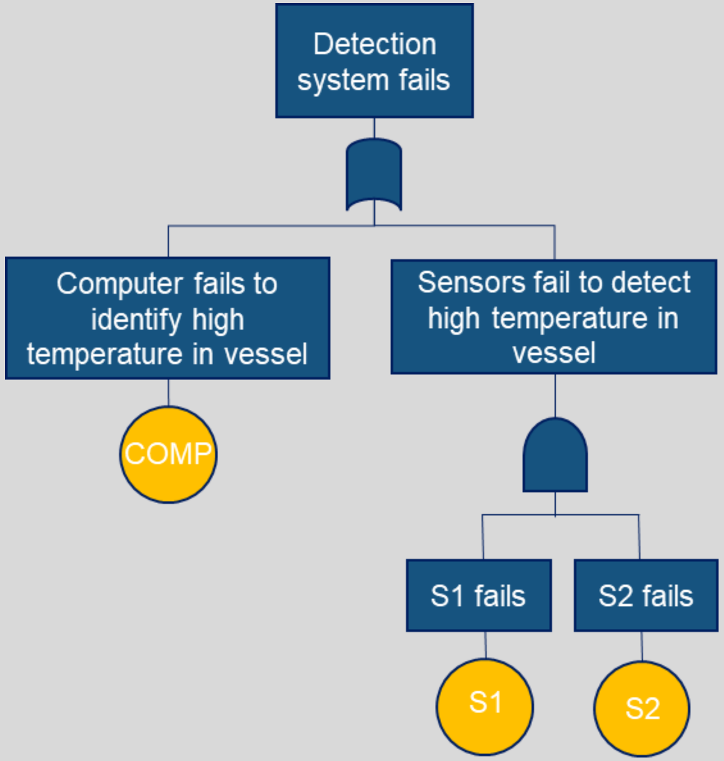
Characterised by non-constant failure and repair rates





Detection System



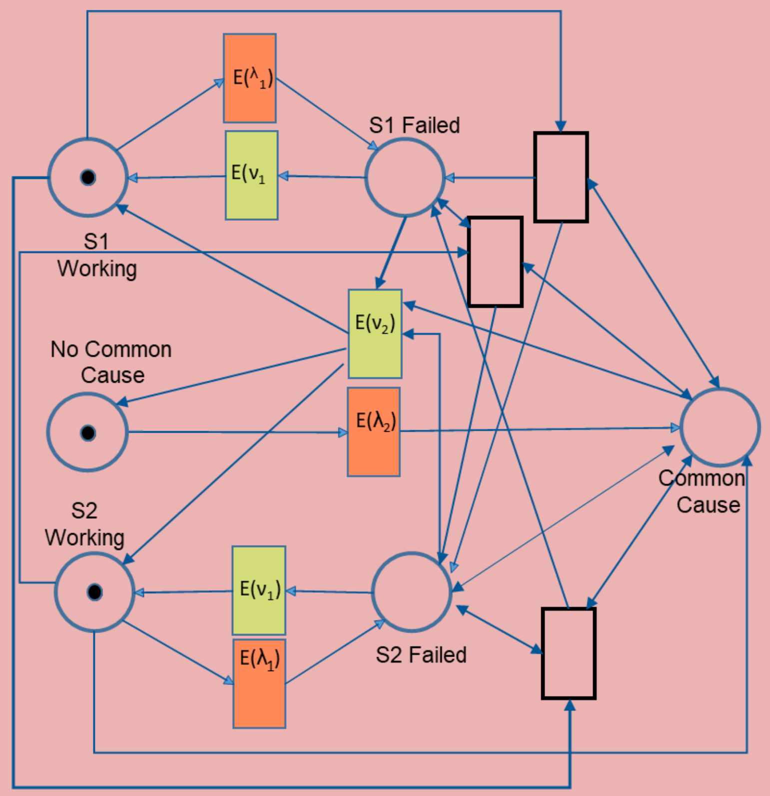


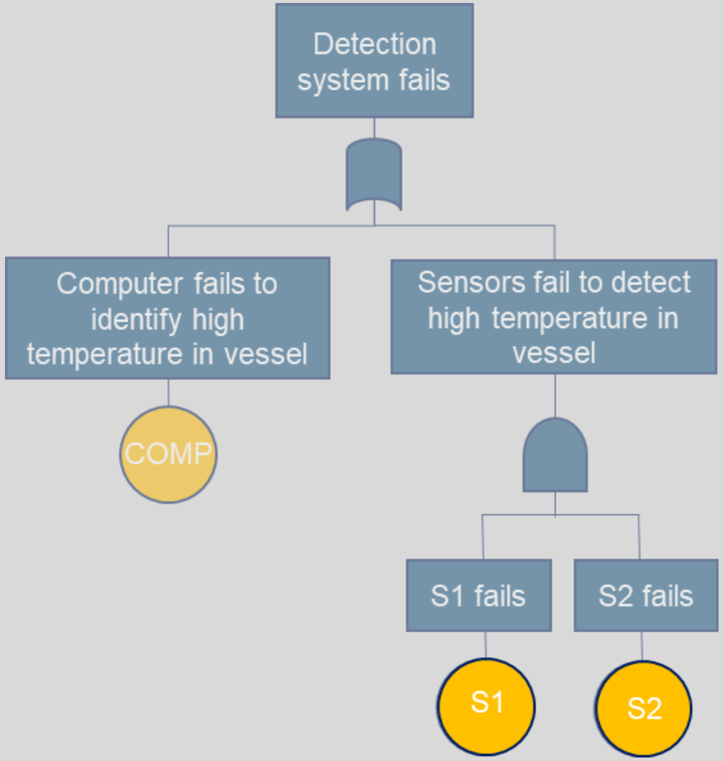
Detection System

S1&S2 Common Cause Failure

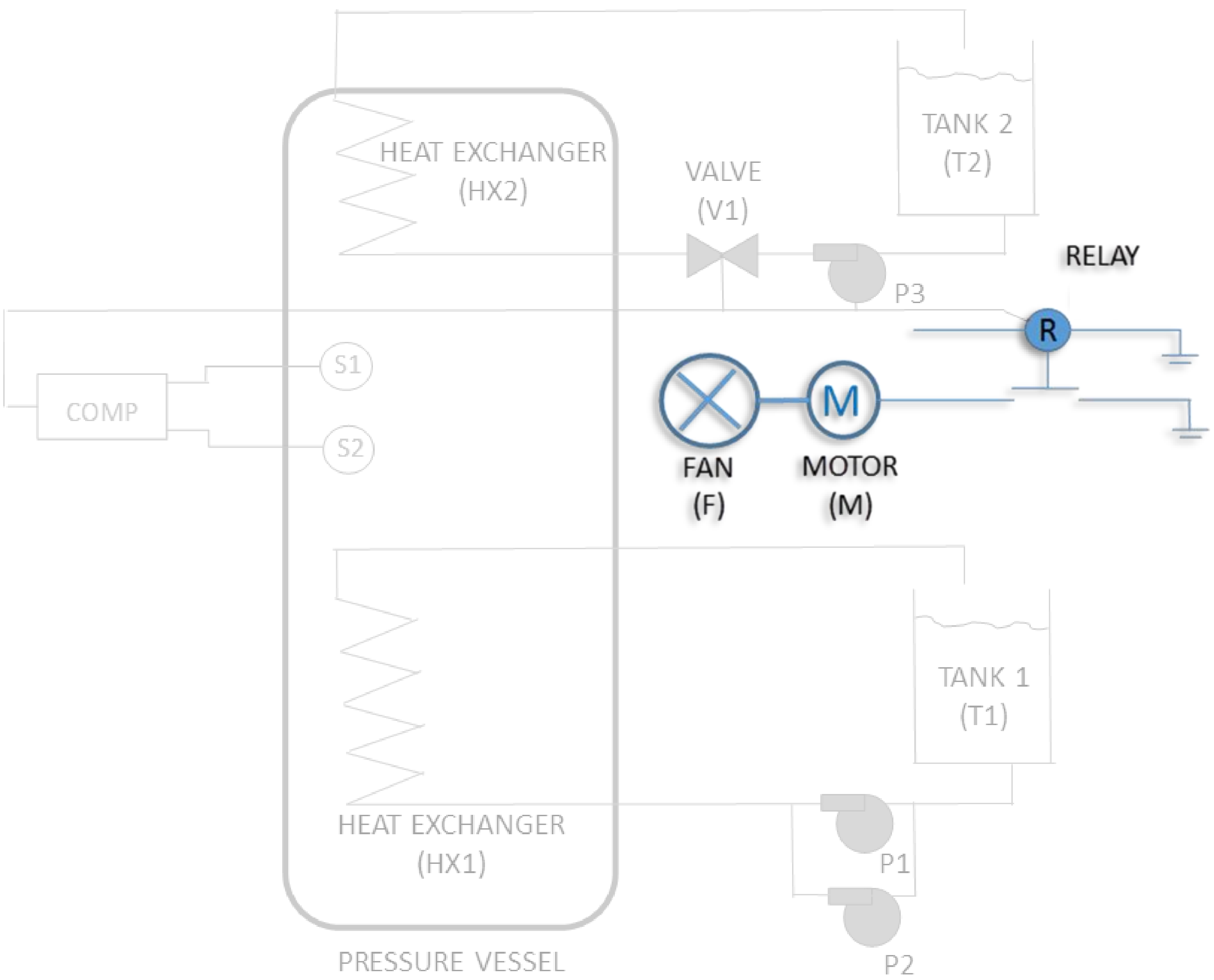
Calibration failure in both sensors when event CC occurs

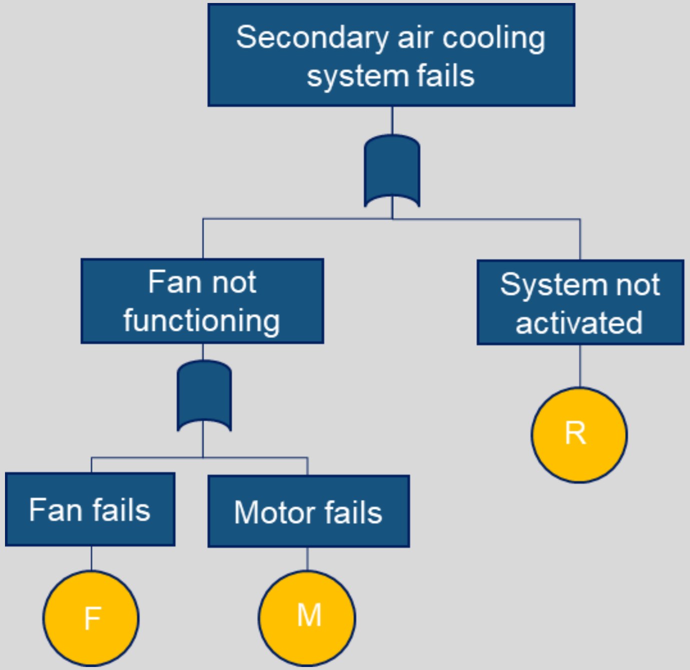
PETRI NET MODEL





Secondary Air Cooling

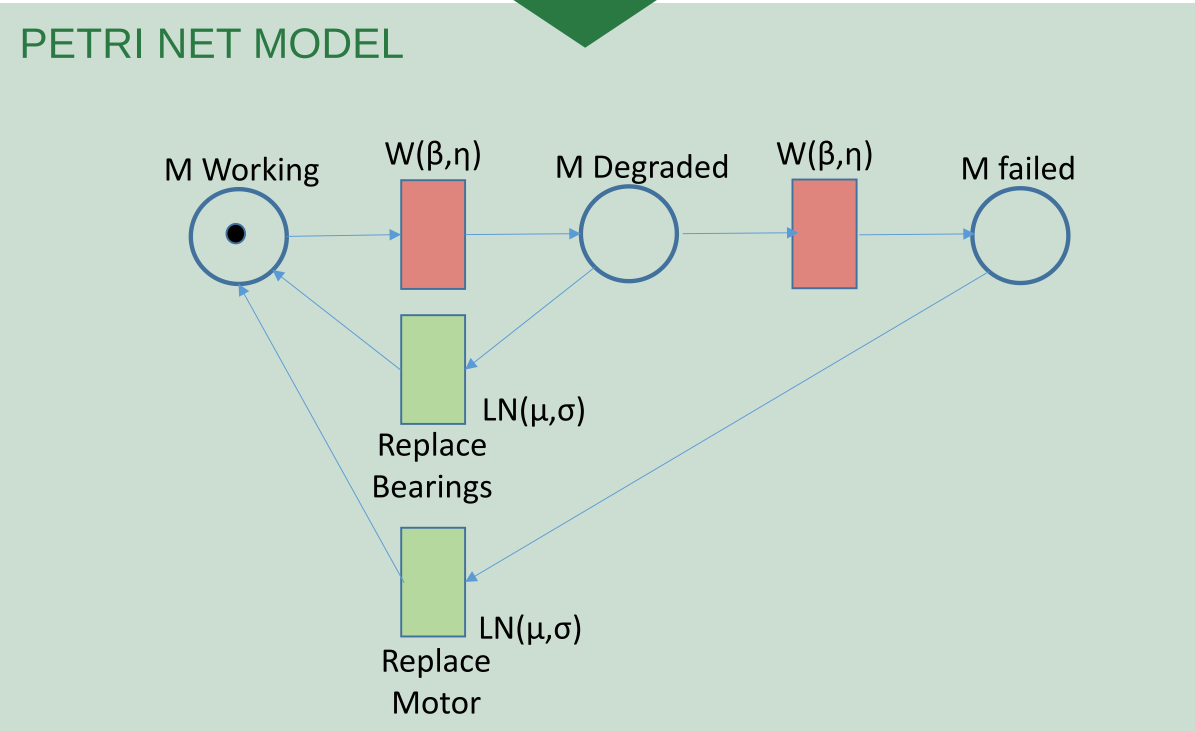


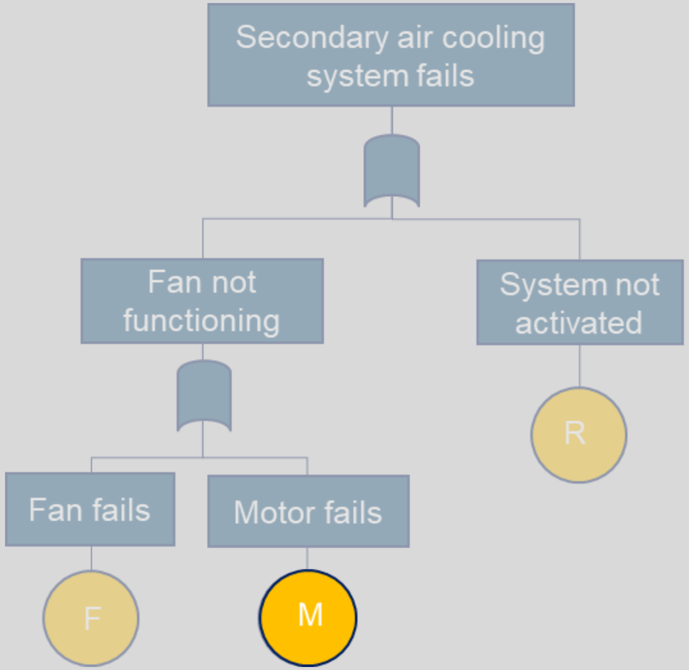


Secondary Air Cooling

M Complex Maintenance Strategy

Condition monitoring system with different maintenance actions





Hands On

Solution

Step 1: Component Reliability

COMPONENTS - Notepad

File Edit Format View Help

```
HX1
FAIL
1.7e-6
REPAIR
0.0417

M
PN
M_PN

P1
DEP

R
FAIL
weibull,2.1,500.0
REPAIR
lognormal,1.0,0.2

P2
DEP

HX2
FAIL
1.7e-6
REPAIR
0.0714
```

Constant Rates?

Y

CONSTANT FAILURE/REPAIR RATES

IDENTIFY MODEL

- Non-Repairable
- **Corrective Maintenance**
- Scheduled Maintenance

COMPUTE RELIABILITY

$$q(HX1) = \frac{\lambda}{\lambda + \nu}$$

$$f(HX1) = \lambda*(1-q(HX1))$$

[λ= failure rate, ν = repair rate]

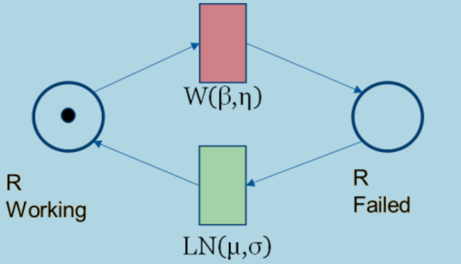
STORE OUTPUT

HX1	
Unavailability	$3.92e^{-3}$
Failure Frequency [h^{-1}]	$1.63e^{-4}$

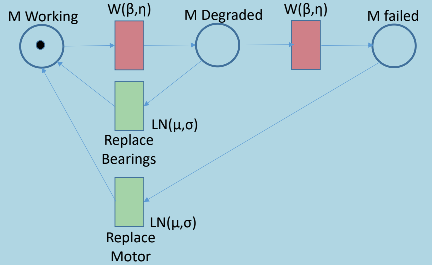
N

NON-CONSTANT FAILURE/REPAIR RATES

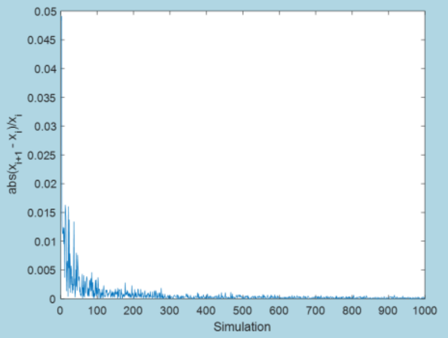
GENERATE PN



INPUT MODEL



RUN TO CONVERGENCE



STORE OUTPUT

R	
Unavailability	$4.22e^{-5}$
Failure Frequency [h^{-1}]	$1.76e^{-6}$

M	
Unavailability	$4.38e^{-3}$
Failure Frequency [h^{-1}]	$1.99e^{-6}$

University of Nottingham
UK | CHINA | MALAYSIA

Step 2: Independent FTs definition

INPUT FTs

PRIMARY - Notepad

```
PRIMARY,1,G1,G2
G2,0,P1,P2
G1,1,HX1,T1
```

SECONDARY_DFT - Notepad

```
SECONDARY,1,F1,R,F1
F2,1,V1,P2
F1,1,HX2,T2
```

DETECTION_FT - Notepad

```
DETECTION,1,K1,COMP
K1,0,S1,S2
```

FAN - Notepad

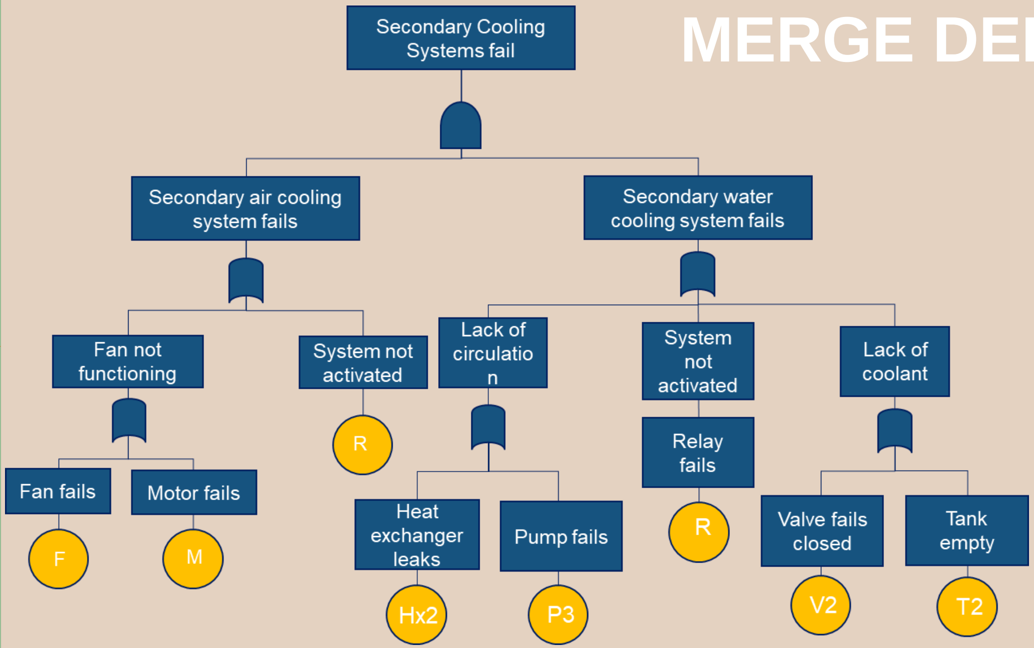
```
FAN,1,R1,H1
H1,1,M,F
```

INDEPENDENT ?

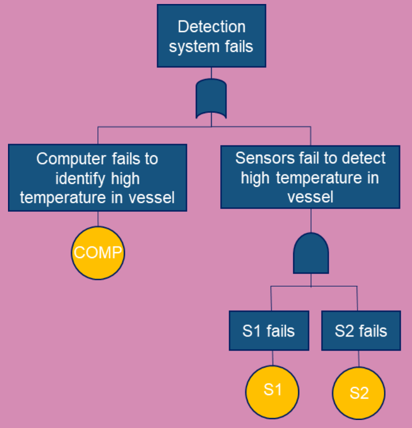
DEPENDENCY - Notepad

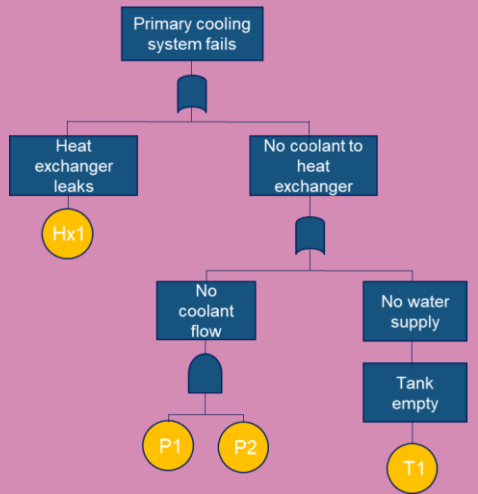
```
MMs
P1P2_MM

MMs
S1S2_MM

SHARED
R:SECONDARY,FAN
```

MERGE DEPENDENT FTs



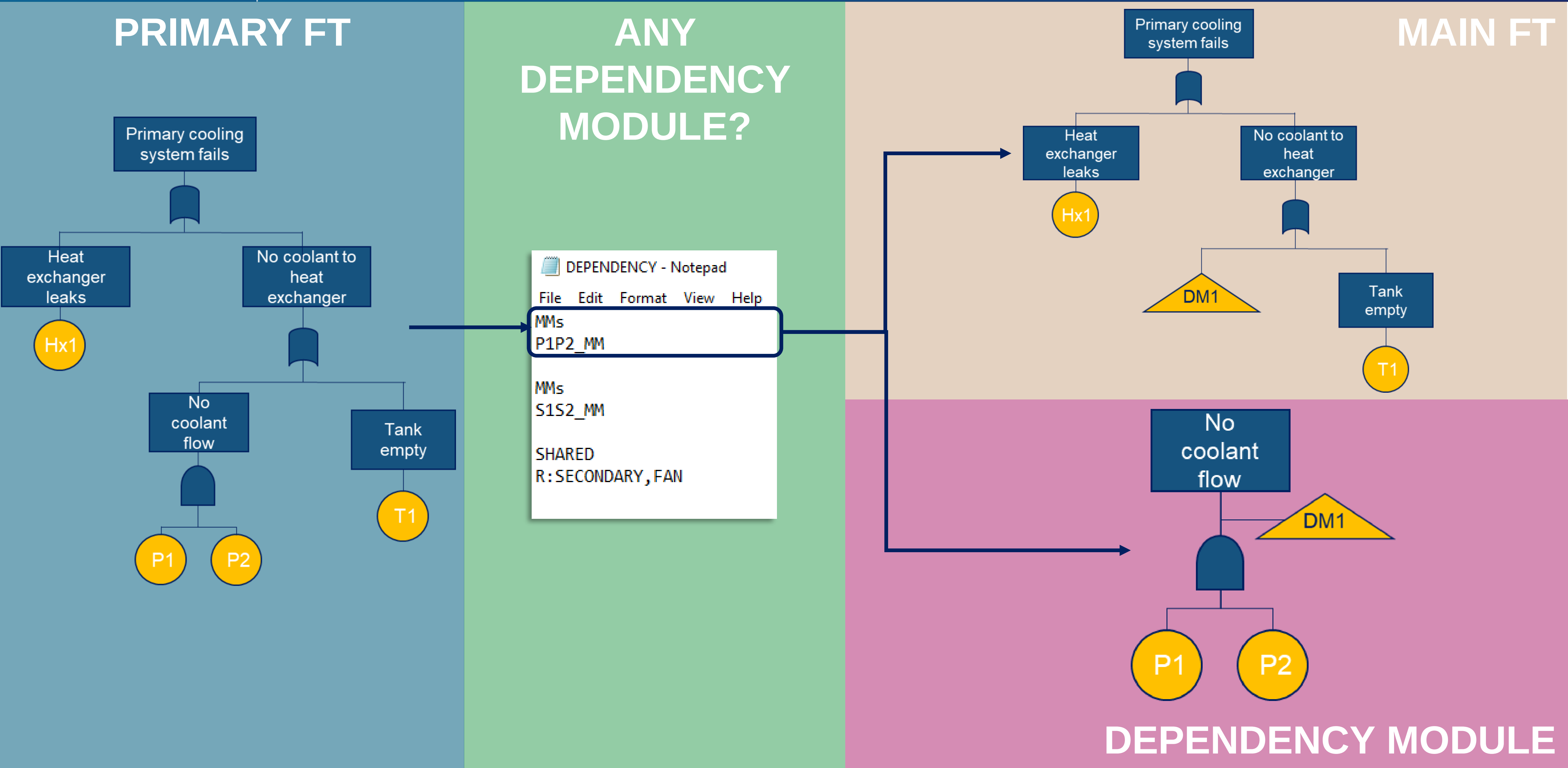
STORE INDEPENDENT FTs



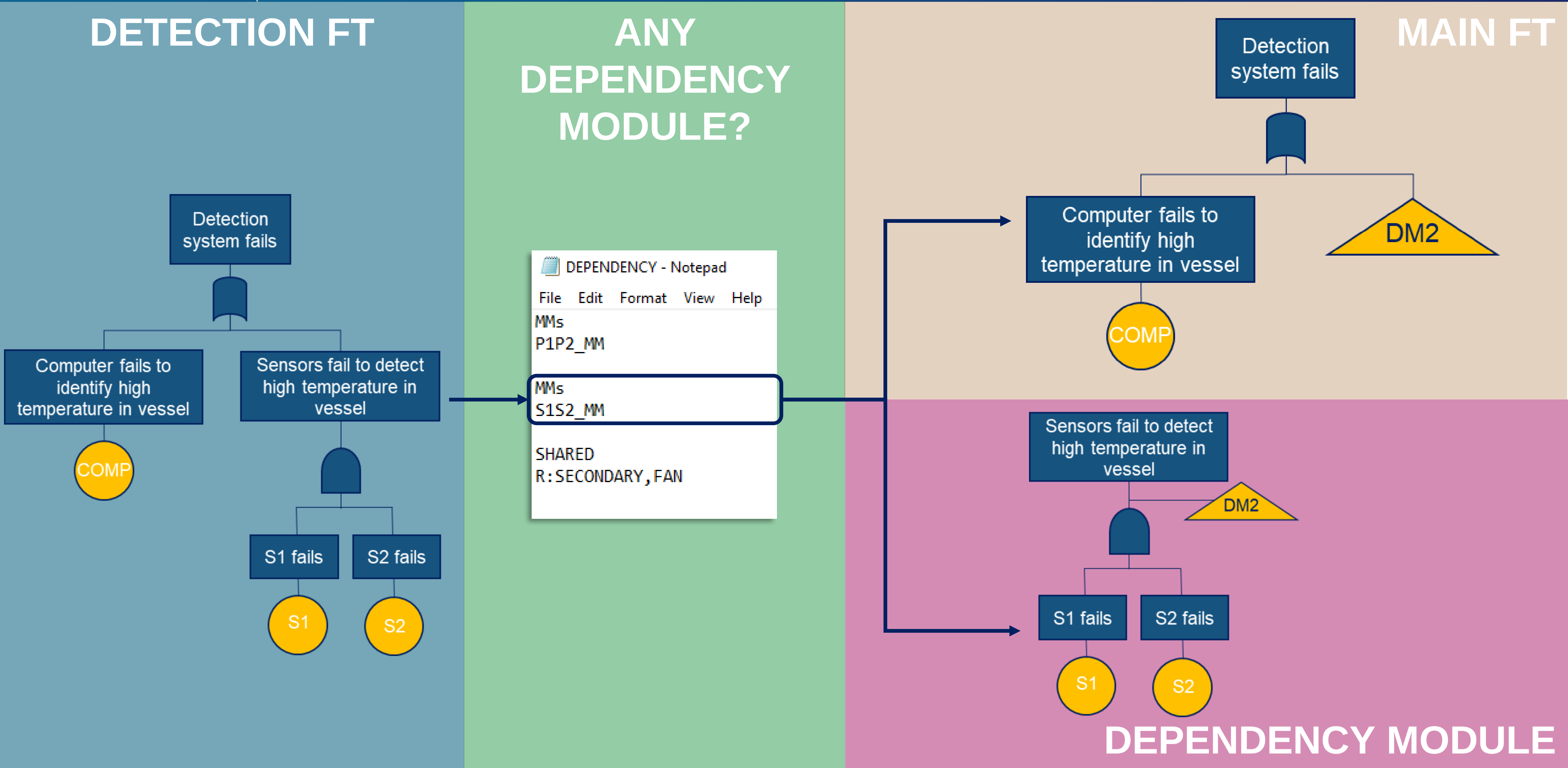


University of Nottingham
UK | CHINA | MALAYSIA

Step 3: Dependency Modules Identification

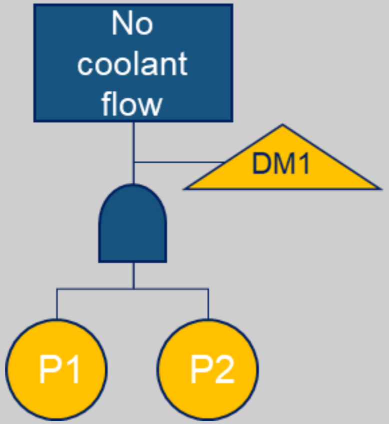


Step 3: Dependency Modules Identification

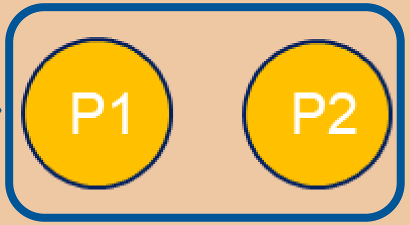


Step 4: Dependency Modules Computation

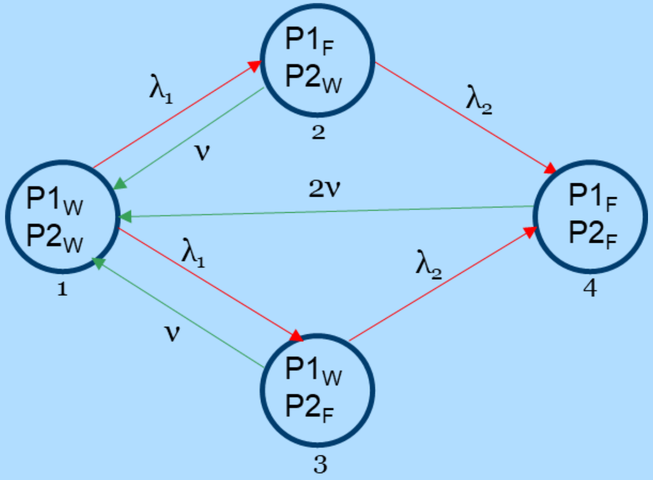
DM 1



DEPENDENCY GROUP



MM MODEL



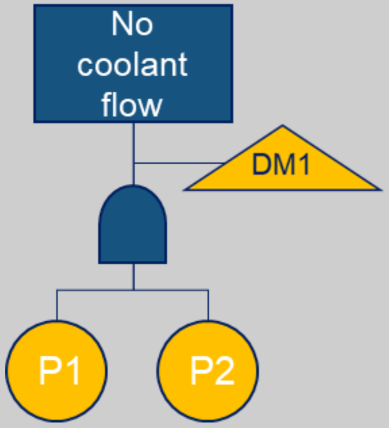
JOINT VALUES

State	Probability	Frequency
$P1_F$,$P2_F$	1.3362e-04	3.3406e-05
$P1_F$,$P2_w$	6.1823e-03	7.8999e-04
$P1_w$,$P2_F$	6.1823e-03	7.8999e-04
$P1_F$,$P2_w$	9.8749E-01	1.5799e-03

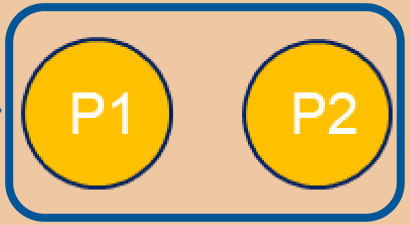
*steady state solution

Step 4: Dependency Modules Computation

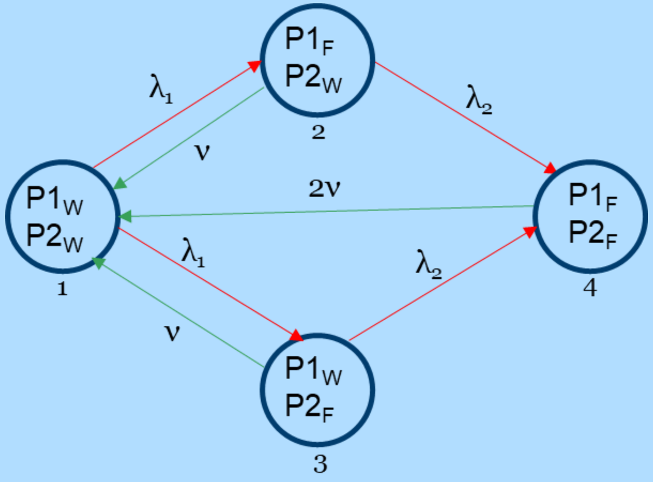
DM 1



DEPENDENCY GROUP



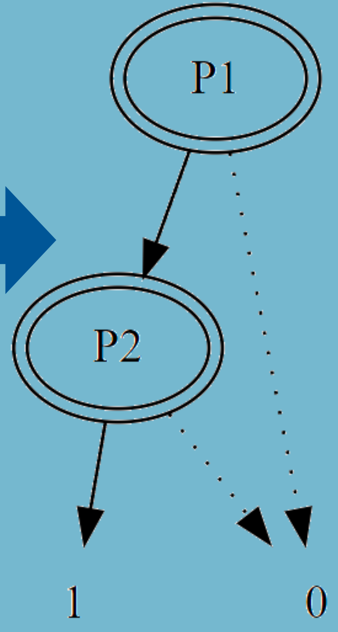
MM MODEL



JOINT VALUES

State	Probability	Frequency
$P1_F$,$P2_F$	1.3362e-04	3.3406e-05
$P1_F$,$P2_W$	6.1823e-03	7.8999e-04
$P1_w$,$P2_F$	6.1823e-03	7.8999e-04
$P1_F$,$P2_W$	9.8749E-01	1.5799e-03

*steady state solution



$$\mathrm{Q(DM1)} = \mathrm{q(P1,P2)} = 1.3362e^{-04}$$

$$\mathrm{F(DM1)} = G(P1)\cdot f(P1) + G(P2)\cdot f(P2) = 3.4792e^{-05}$$

$$G(P1) = \mathrm{Q(DM1|P1)} - \mathrm{Q}(\mathrm{DM1}|\overline{P1})$$

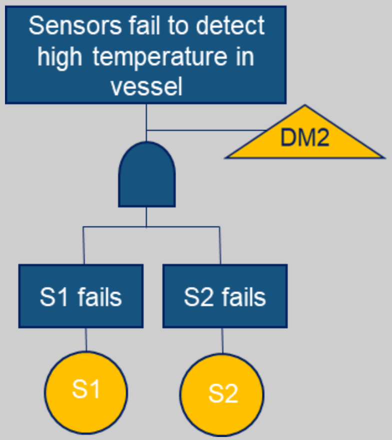
$$G(P2) = \mathrm{Q(DM1|P2)} - \mathrm{Q}(\mathrm{DM1}|\overline{P2})$$

Birnbaum's Measure of Importance

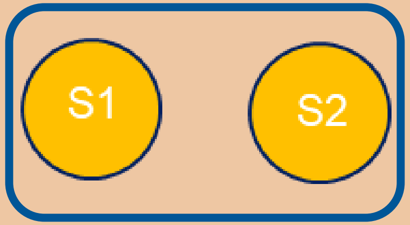
BDD CALCULATION

Step 4: Dependency Modules Computation

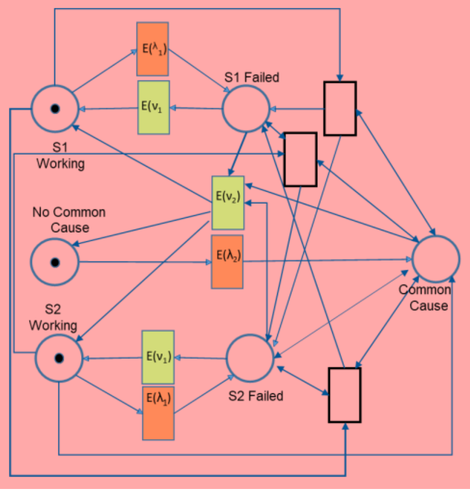
DM 2



DEPENDENCY GROUP



PN MODEL

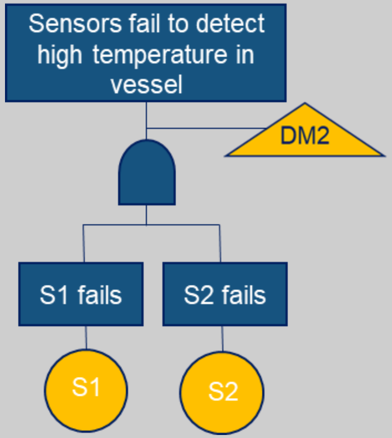


JOINT VALUES

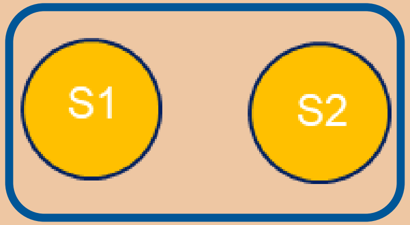
State	Probability	Frequency
$S1_F,S2_F$	4.8023e-04	5.1446e-05
$S1_F,S2_W$	3.3018e-06	1.5221e-06
$S1_W,S2_F$	4.4003e-06	1.4459e-06
$S1_W,S2_W$	9.9951e-01	5.4414e-05

Step 4: Dependency Modules Computation

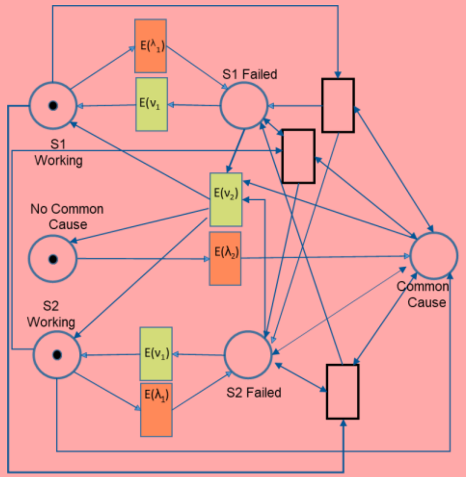
DM 1



DEPENDENCY GROUP

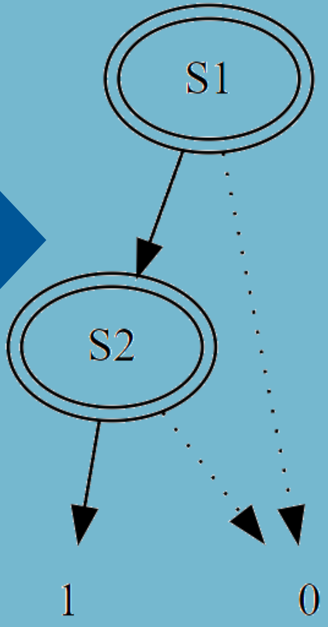


PN MODEL



JOINT VALUES

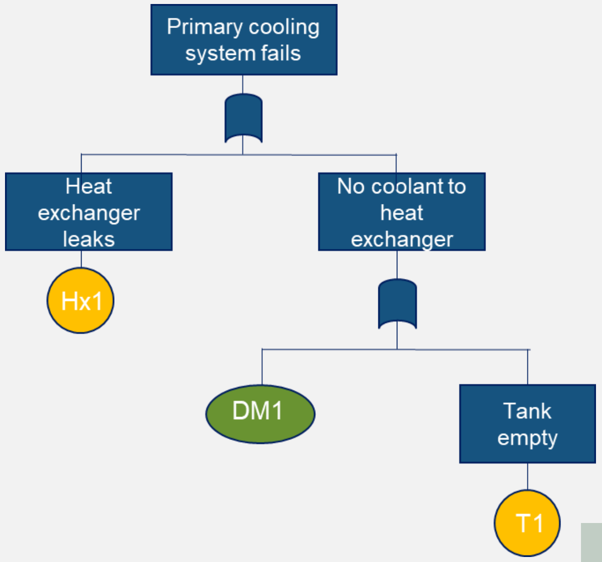
State	Probability	Frequency
$S1_F, S2_F$	4.8023e-04	5.1446e-05
$S1_F, S2_W$	3.3018e-06	1.5221e-06
$S1_W, S2_F$	4.4003e-06	1.4459e-06
$S1_W, S2_W$	9.9951e-01	5.4414e-05

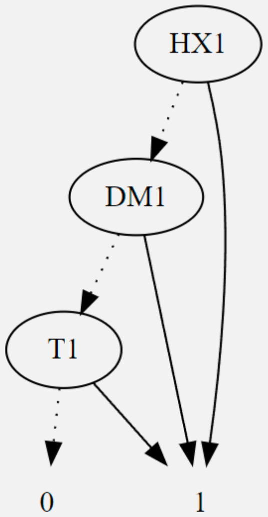


$$Q(DM2) = q(S1,S2) = 4.8023e^{-04}$$

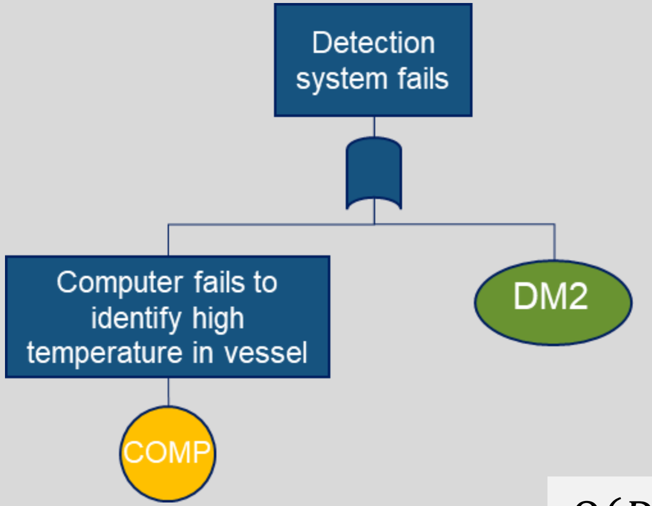
BDD CALCULATION

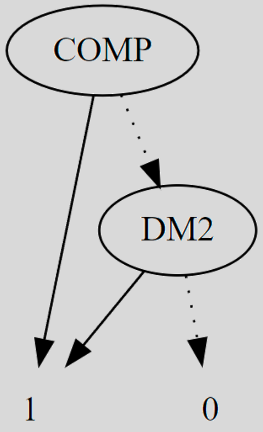
Step 5: FTs Computation



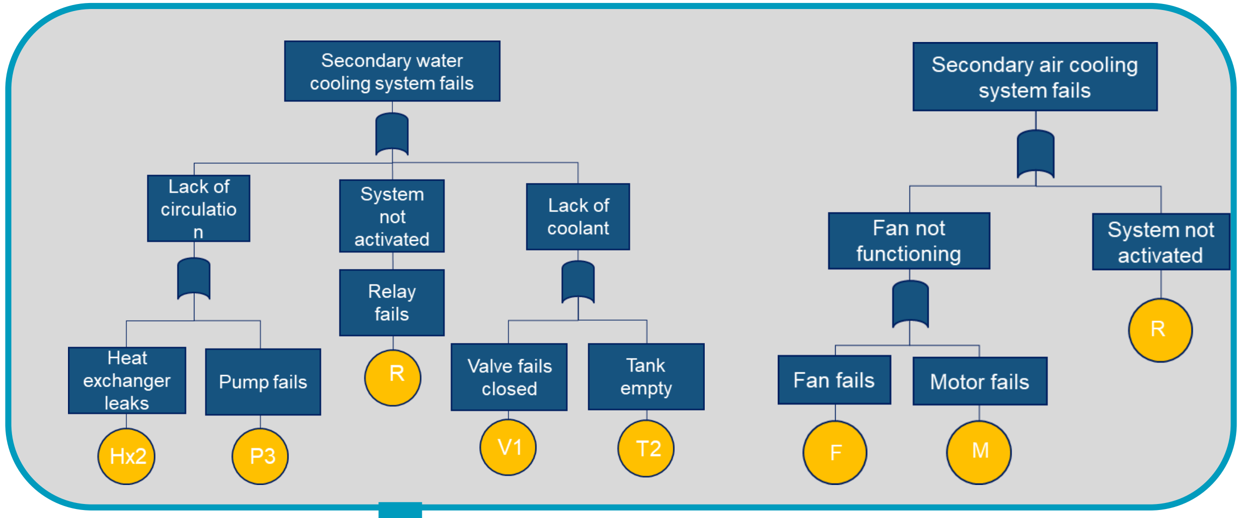


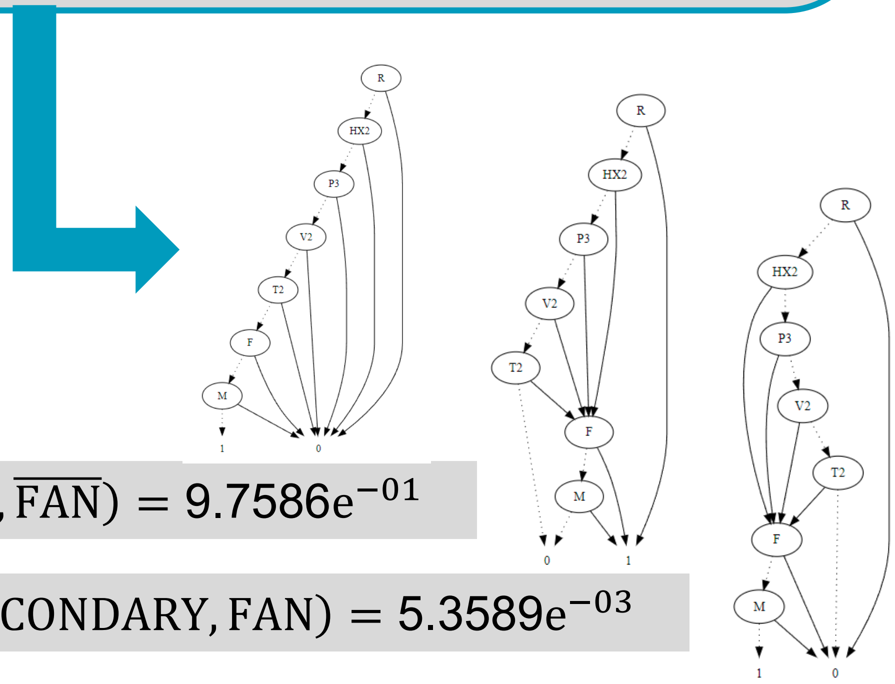
$$Q(PRIMARY) = 1.7460e^{-04}$$





$$Q(DETECTION) = 7.1802e^{-03}$$





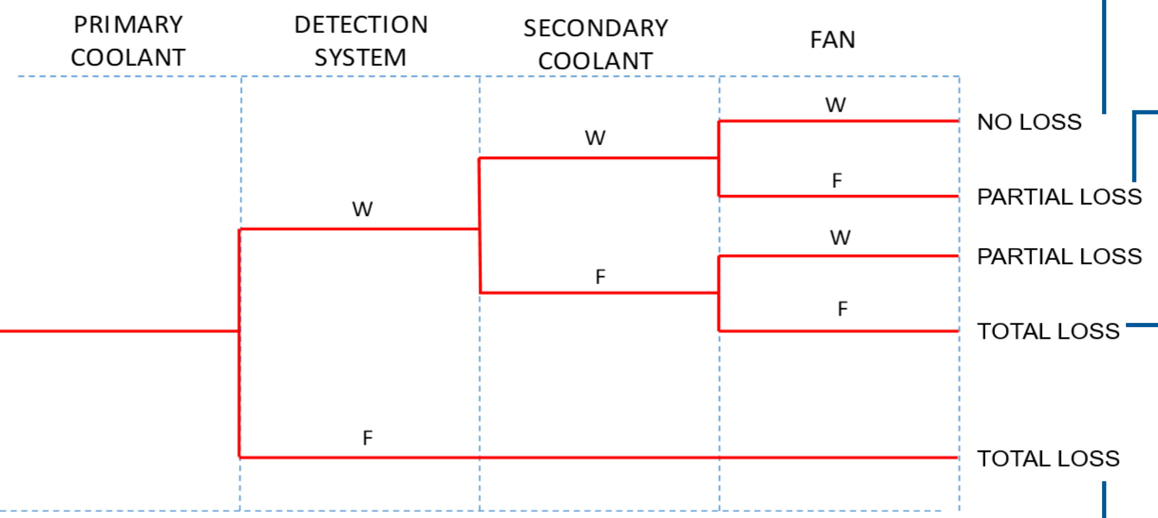
$$Q(\overline{SECONDARY}, \overline{FAN}) = 9.7586e^{-01}$$

$$Q(SECONDARY, FAN) = 5.3589e^{-03}$$

$$Q(SECONDARY, \overline{FAN}) = 5.3589e^{-03}$$

University of Nottingham
UK | CHINA | MALAYSIA

Step 6: ET Computation



$$f_{NoLoss} = f_{primary} \cdot q(\overline{Detection}) \cdot q(\overline{Fan}, \overline{Secondary}) = 3.5770e^{-05}$$

$$f_{PartialLoss1} = f_{primary} \cdot q(\overline{Detection}) \cdot q(Fan, \overline{Secondary}) = 4.6184e^{-07}$$

$$f_{PartialLoss2} = f_{primary} \cdot q(\overline{Detection}) \cdot q(\overline{Fan}, Secondary) = 1.9643e^{-07}$$

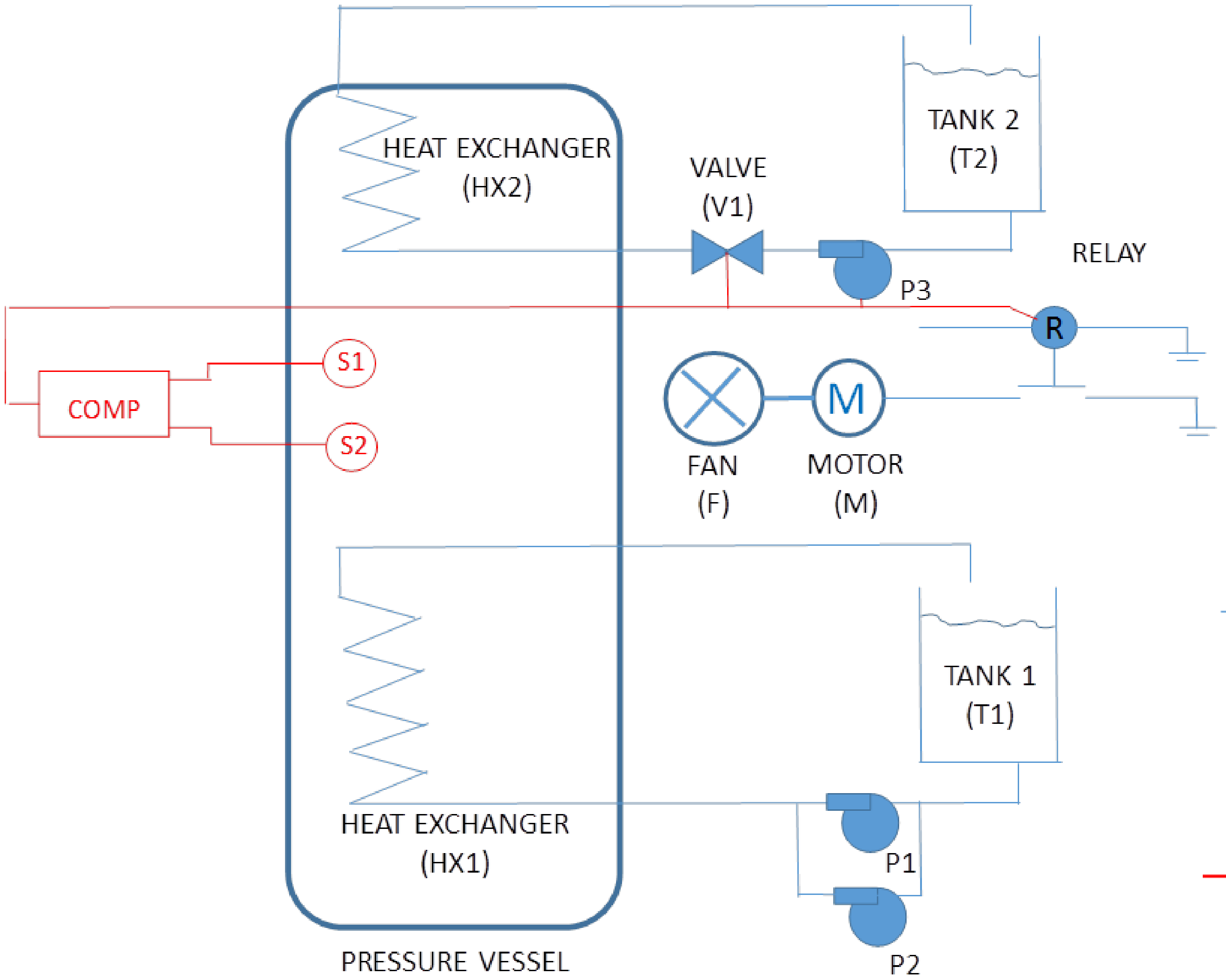
$$f_{TotalLoss1} = f_{primary} \cdot q(\overline{Detection}) \cdot q(Fan, Secondary) = 2.2664e^{-07}$$

$$f_{TotalLoss2} = f_{primary} \cdot q(Detection) = 2.6509e^{-07}$$

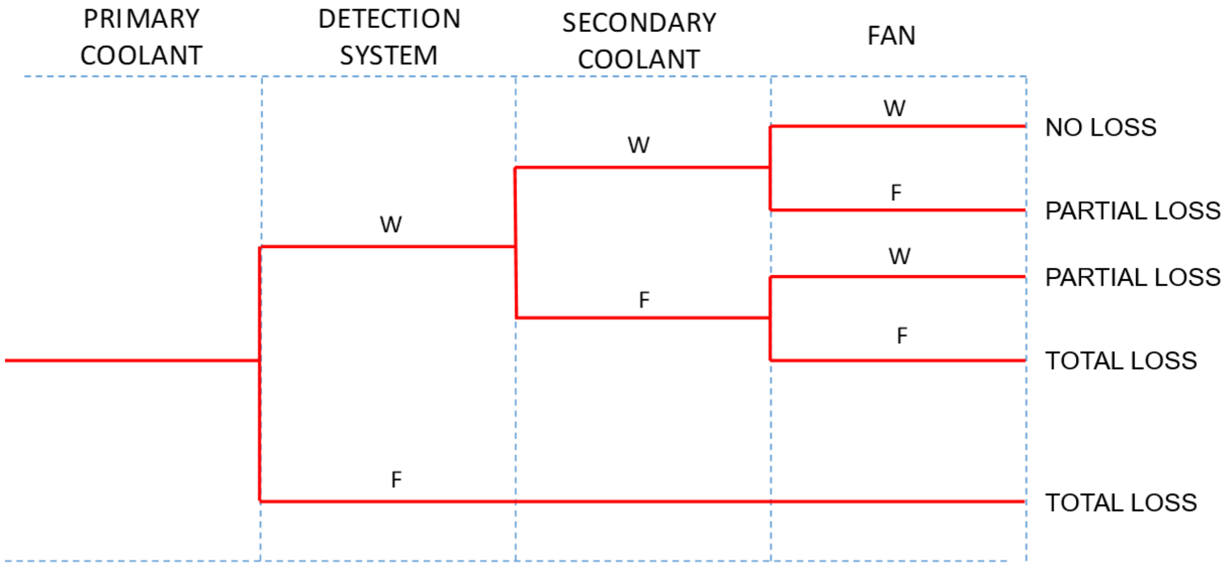
$$q(Fan, \overline{Secondary})$$
$$= q(\overline{Secondary}) - q(\overline{Fan}, \overline{Secondary})$$

$$q(\overline{Secondary})$$
$$= 1 - q(\overline{Fan}, Secondary) - q(Fan, Secondary)$$

Results



Loss of Cooling	Frequency [h^{-1}]
None	$3.5770e^{-05}$
Partial	$6.5614e^{-07}$
Total	$4.9173e^{-07}$



Summing Up

Conclusions

University of Nottingham
UK | CHINA | MALAYSIA

Conclusions

- System safety discipline born to tackle challenges introduced by increasing systems complexity
- Today's systems present further challenges, for instance their intrinsic dynamic nature (automation and control), complex maintenance strategies (e.g. condition monitoring) and ageing (for older system)
- Traditional system safety techniques have strong limitations in modelling these complexities
- Assumptions common to traditional approaches (e.g. component independence and failure rate constancy) may result in the under-estimation of risk or over-conservatism
- Available simulation-based techniques provide the required modelling flexibility but do not guarantee computational feasibility for large-scale systems

Conclusions

- The integration of more flexible modelling techniques with traditional system safety methodologies (such as FT/ET, BDD) can tackle these challenges
- The proposed umbrella methodology aims at maintaining the familiar modelling language well rooted in the engineering community
- It allows to model accurately complex features of engineering systems (e.g. components dependencies, degradation and complex maintenance strategies) through the use of modelling techniques such as PNs and MMs…
- …while maintaining a traditional FT/ET approach for the remaining sections of the system for which traditional assumptions are justified

University of Nottingham
UK | CHINA | MALAYSIA

Thank you

silvia.tolo@nottingham.ac.uk