FAULT TREE ANALYSIS (FTA)

1. Fault tree analysis: objectives and construction rules
2. A case study: Fire detector system
3. Qualitative and Quantitative Assessments
4. Conclusions
5. Exercices

Fault Tree : Objectives

Search the different *possible combinaisons* of events which can **cause *the critical event***: **Hazardeous** scenarios.

Graphical representation of these combinaisons with a *tree logical structure*.

Study of a Fault Tree can lead to:

- Qualitative Analysis
  - A better understanding of the failure mechanism of a complex system
  - Illustration of the common cause failures
  - opportunities to reveal and correct some system weakness - develop *barriers* or/and *protective systems* ⟹ Depth-defense
- Quantitative Analysis:
  - Evaluation of the *probability* of the the occurrence of the top event
  - Reliability, Availability and Safety Measures

Probabilistic importance measures

Fault tree analysis process

6 steps :

1 Definition of the problem and the boundary conditions

2 Construction of the Fault Tree

3 Identification of the minimal cut and/or path sets

4 Qualitative Analysis of the fault tree

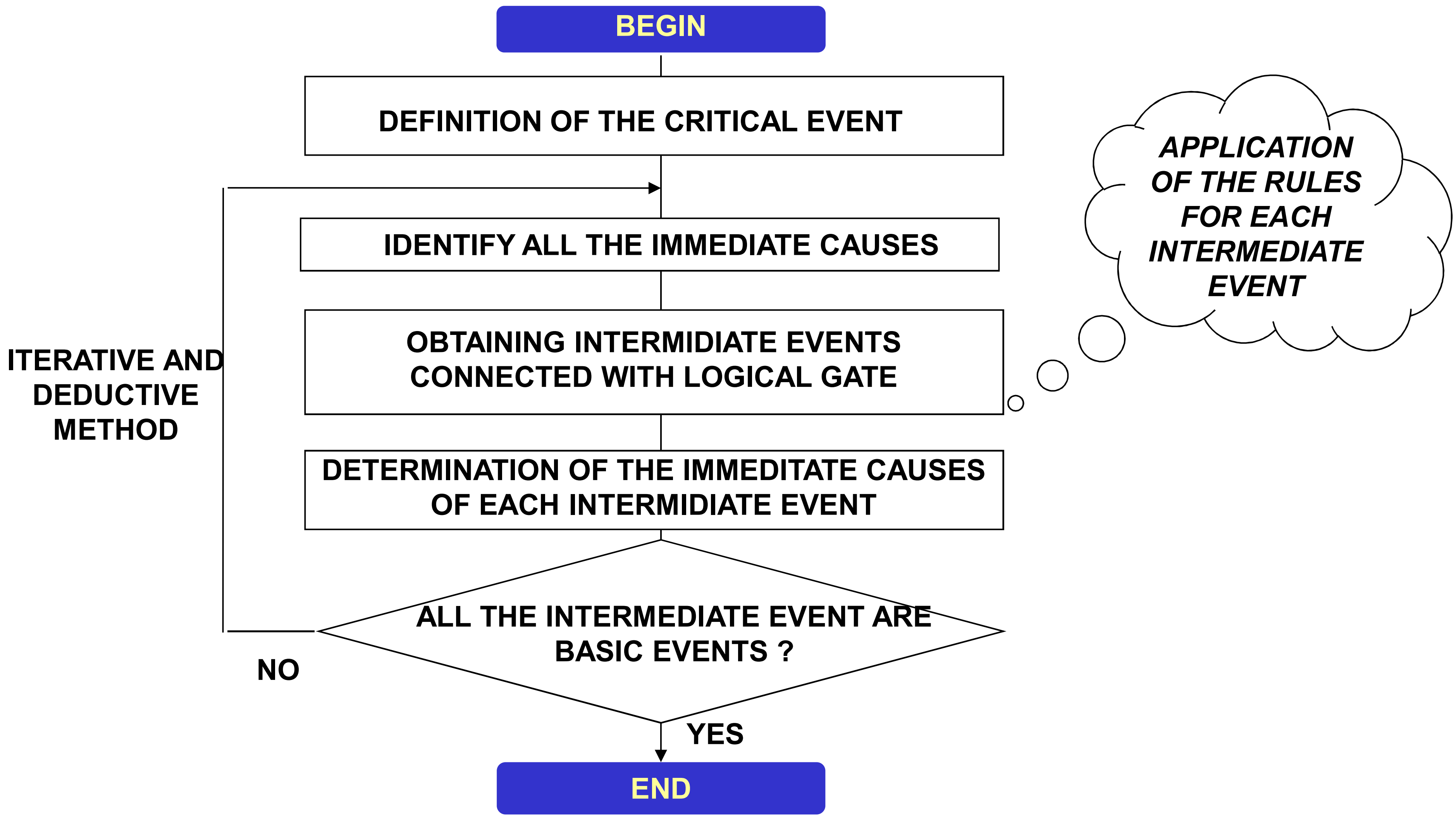
5 Quantitative Analysis of the fault tree

6 Definition of the potential action plans or improvements

Step 1. Problem & boundary conditions

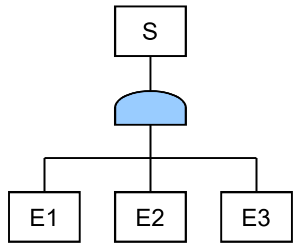
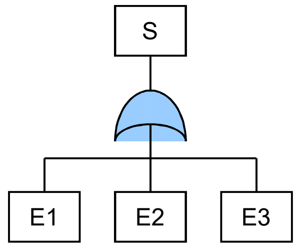
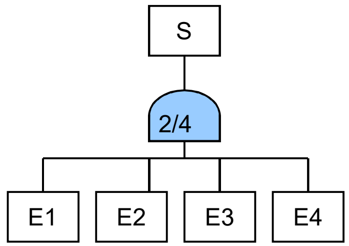
- Definition of the critical event (the accident) = the TOP event:
  - WHAT: type of critical event (fire)
  - WHERE: place of the critical event (in the process oxydation reactor)
  - WHEN: time of the critical event (during normal operation)
- Definition of the boundary conditions:
  - **Physical boundaries of the system**. What parts of the system?
  - **The initial conditions**
    - What is the operational state of the system when the TOP event is occurring ?
    - Is the system running on full/reduced capacity ?
    - Which valves are open/closed, which pumps are functionning ?, etc.
  - **Boundary conditions**. type of external stresses (sabotage, earthquake, lightning,etc.) in the analyses ?
  - **The level of resolution**
    - How far down in detail should go to identify potential reasons for a failed state ? (« valve failure » ? Or failures in the valve housing, stem, actuator ? Or ...)

Step 2. Construction

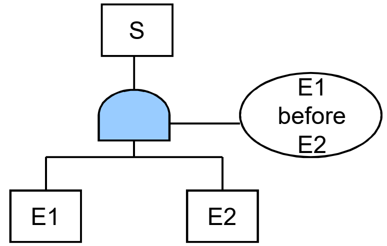
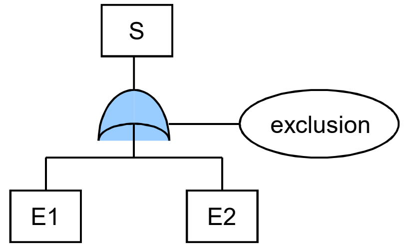
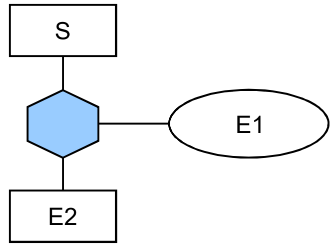


Step 2. Construction

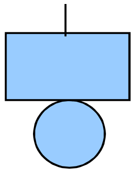
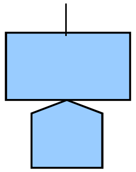
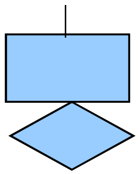
Logic gates

Symbol	Name	Description
	AND-gate	The AND-gate indicates that the output event S occurs only when all the input events Ei occur simultaneously.
	OR-gate	The OR-gate indicates that the ouput event S occurs if any of the input events Ei occur.
	K/N-gate (e.g., 2/4)	The K/N-gate indicates that the output event S occurs only when at least K input events Ei among N occur (e.g., 2 among 4)

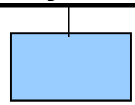
Conditional logic gates

Symbol	Name	Description
	AND-gate with condtion	The AND-gate with condition indicates that the output event S occurs only when all the input events Ei occur with the condition (E1 before E2).
	Exclusive OR-gate	The exclusive OR-gate indicates that the ouput event S occurs if only one of the input events Ei occur (only E1 or E2).
	Inhibit gate	The inhibit gate indicates that the output event S occurs if both the conditional event E1 and the input event E2 occur.

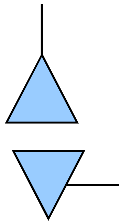
Input events

Symbol	Name	Description
	BASIC event	The Basic event represents a basic equipment fault or failure that requires no further development into more basic faults or failures.
	HOUSE event	The House event represents a condition of an event which is TRUE (ON) or FALSE (OFF) (not true).
	UNDEVEL OPED event	The Undeveloped event represents a fault that is not examined further because information is unavailable or because its consequence is insignificant

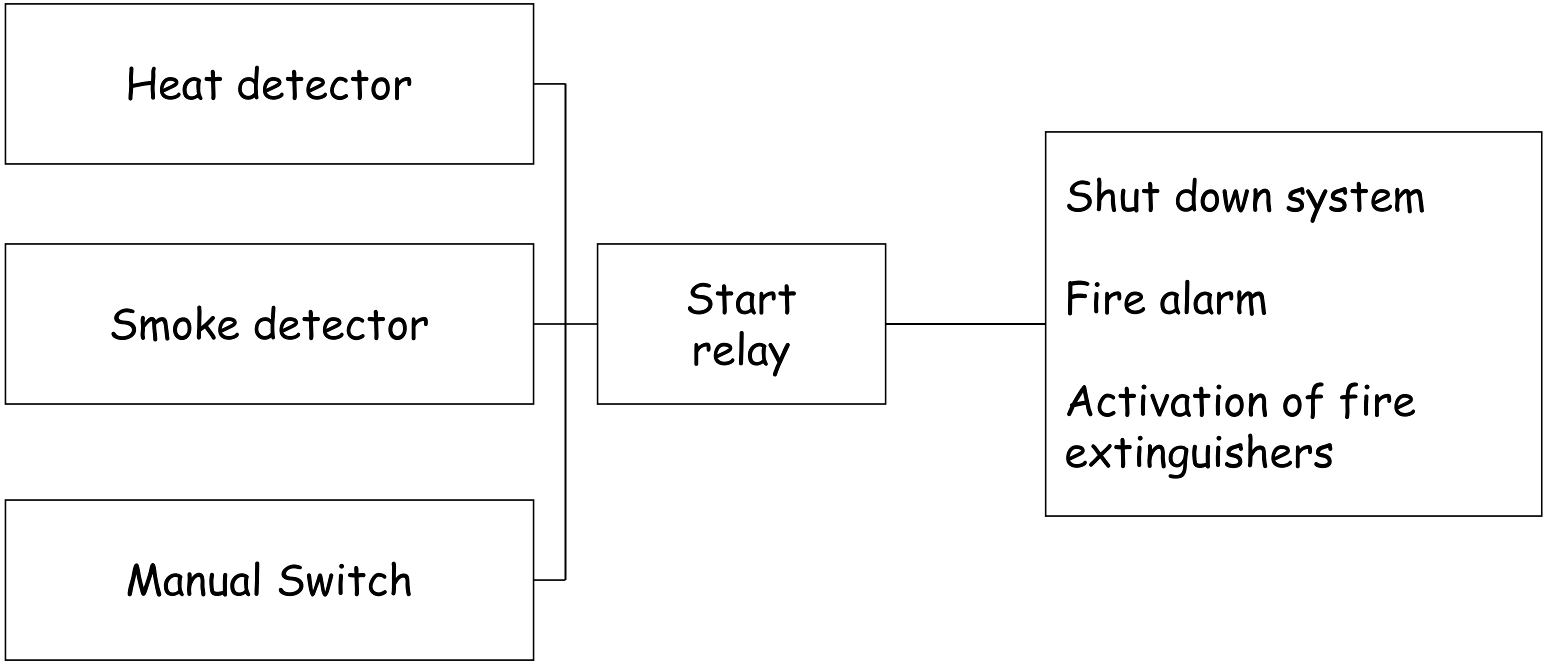
Description of State

Symbol	Name	Description
	COMMENT rectangle	The Comment rectangle is for supplementary information.

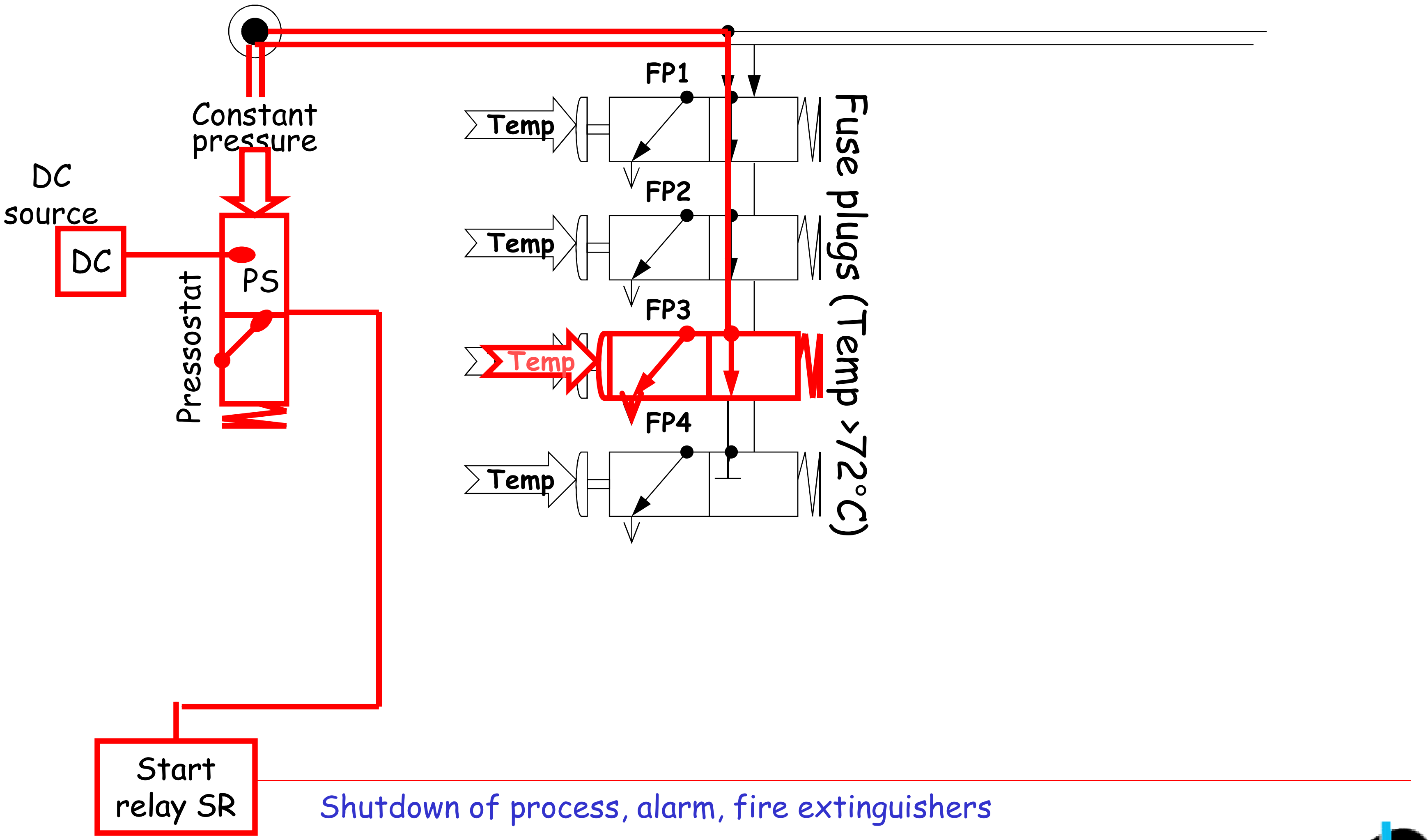
Transfert symbol

Symbol	Name	Description
	TRANSFERT down and TRANSFERT up	The Transfert down symbol indicates that the fault tree is developed further at the occurrence of the corresponding Transfert up symbol

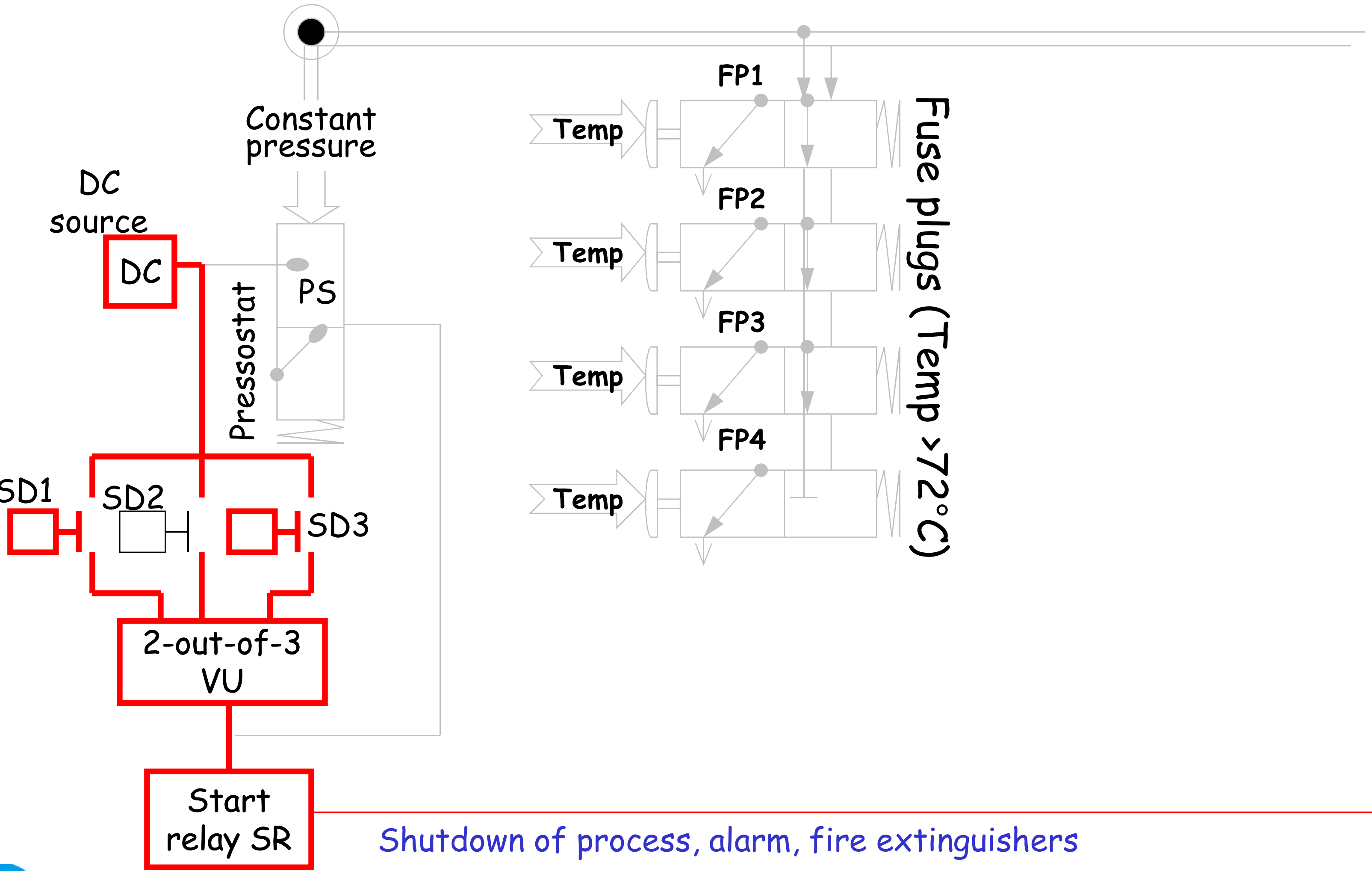
Ex1: Fire detector system



Heat Detection

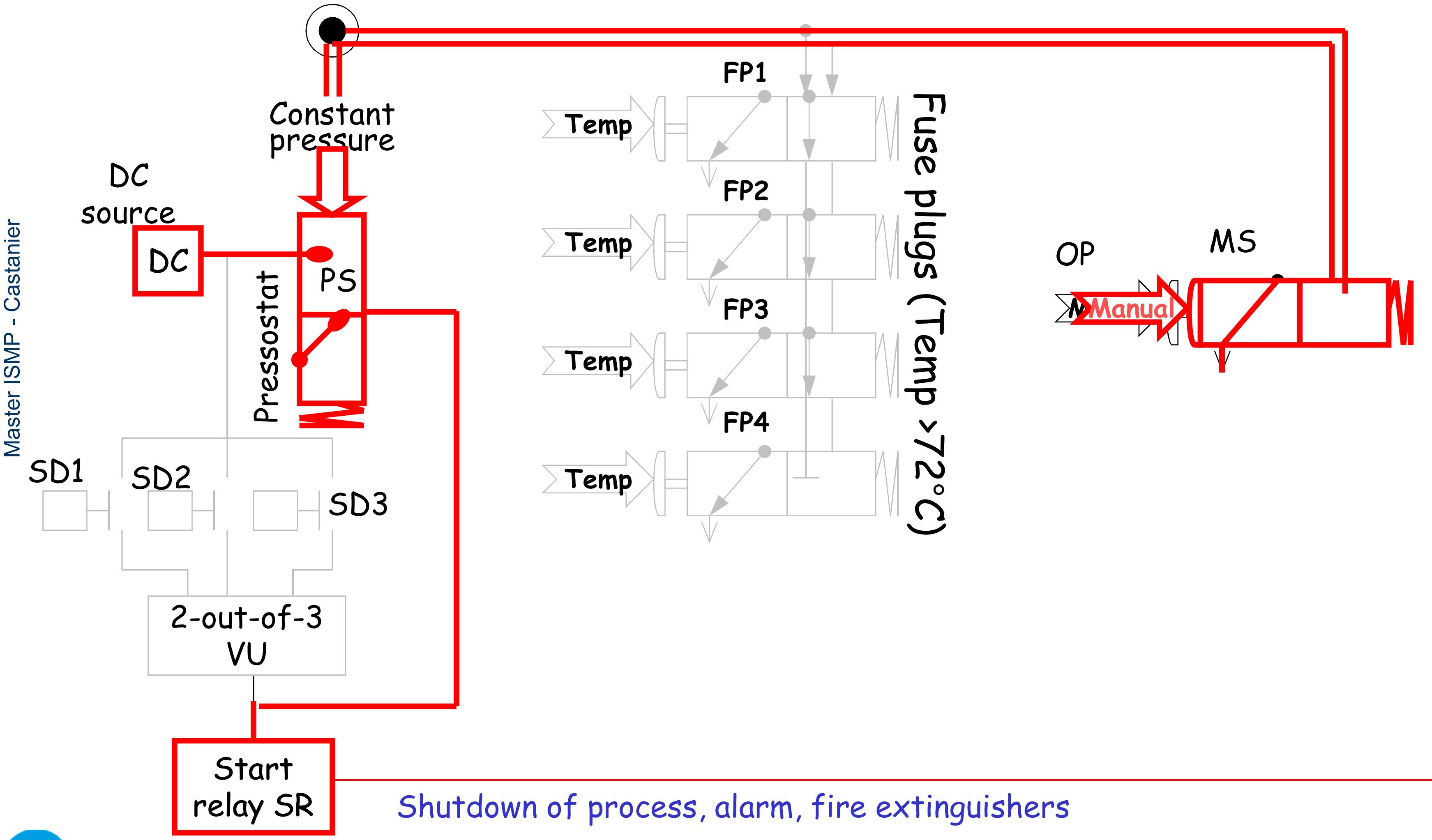


Smoke Detection



Shutdown of process, alarm, fire extinguishers

Manual activation



Shutdown of process, alarm, fire extinguishers

Cut Set:

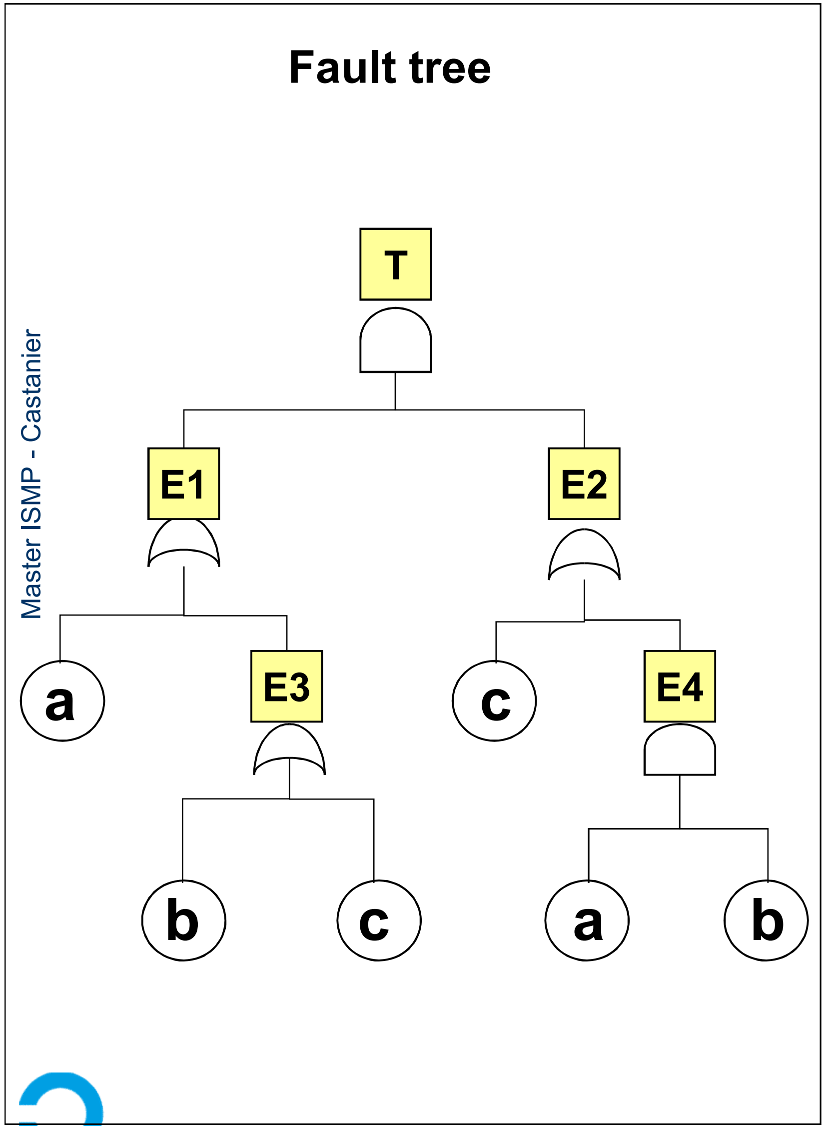
- A *cut set* in a fault tree is a set of basic events whose (simultaneously) occurrence ensures that the TOP event occurs.
- A cut set is said to be *minimal* if the set cannot be reduced without losing its status as a cut set.
- The number of different basic events in a minimal cut set is called the *order* of the cut set.

Path Set:

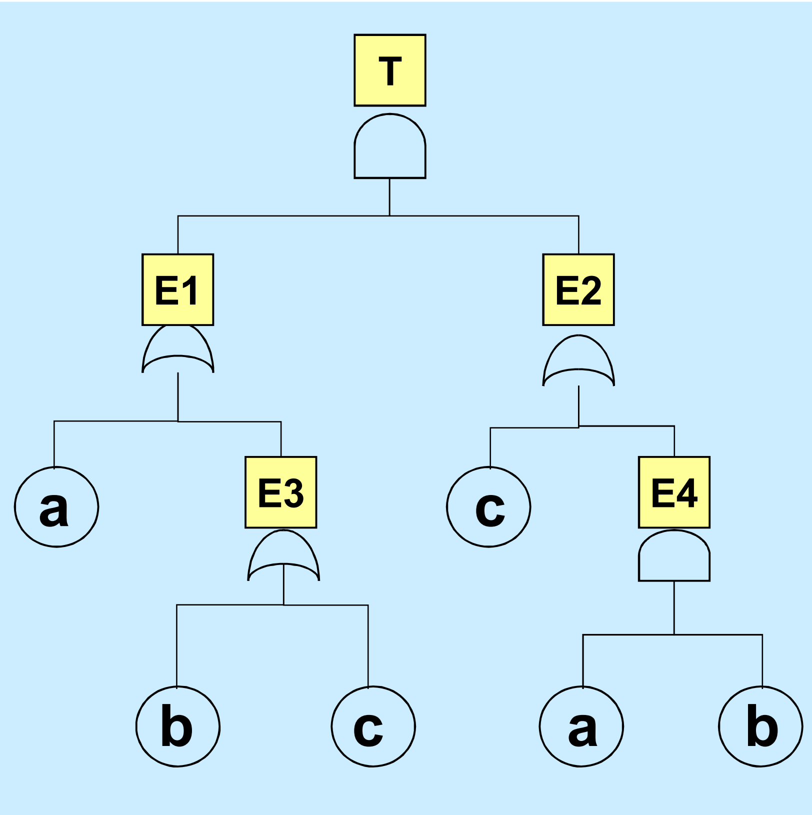
- A *path set* in a fault tree is a set of basic events whose nonoccurrence (simultaneously) ensures that the TOP event does not occur.
- A path set is said to be *minimal* if the set cannot be reduced without loosing its status path set.

Methodology to identify minimal cut set: **Boolean Algebra**

Identification of the minimal cut sets



Arbre de défaillance



Associated Boolean Expression

Intermediate events

E3 = b + c

E1 = a + (b + c) = a + b + c

E4 = a . b

E2 = c + (a . b)

ABSORPTION

❶ : A or A = A

❷ : (A and B) or B = B

Critical Top event

T = E1. E2 = (a + b +c) . (c + (a . b))

T = (a + b + c) . c + (a + b + c) . (a . b)

T = a . c + b . c + c + a . b + a . b + c . a . b

❷ ❶

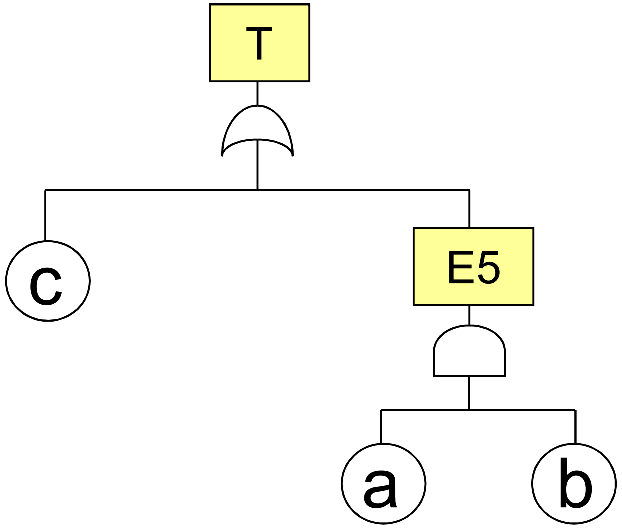
T = a . c + c + a . b + c . a . b

❷ ❷

T = c + a . b

T = c + a . b ⇒ **Reduced tree**

Reduced Fault Tree

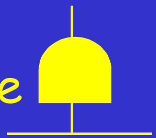
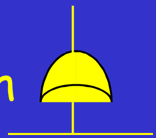


Minimal cut

- The fault tree composed only by the minimal cut sets is called the **« reduced tree ».**
- The minimal cut sets are {c} and {a, b}:
  - {c} (order 1)
  - {a, b} (order 2)
- a, b and c are independent
- The minimal cut sets are the **critical hazardeous scenarios.**

Identification of the minimal path sets

Construction of the **dual fault tree**

Replacing all the  gates with  gates and vice-versa

Identification of the minimal path sets

The same approach than for the minimal cut sets.

Qualitative Risk Assessment (QRA) based on the evaluation of criticality of the minimal cut sets.

Criticality of a minimal cut set depends on:

- *The order of the cut set*
- *The type of the cut set*

To rank the Criticality Minimal Cut Sets

Rank	Type of Basic Event
1	Human error (HE)
2	Active equipment failure (AEF)
3	Passive equipment failure (PEF)

Rank	Basic event 1	Basic event 2
1	HE	HE
2	HE	AEF
3	HE	PEF
4	AEF	AEF
5	AEF	PEF
6	PEF	PEF

Quantitative Analysis

System reliability measure	Description
$Q_0(t)$	The probability that the TOP event occurs at time *t*
$R_0(t)$	The probability that the TOP event does not occur in [0,t)
MTTF	Mean time to first system failure
Freq distr.	Distribution of TOP event frequency
Freq(TOP)	Frequency of the TOP event
E(#failures)	Expected number of failures within a time period
$A_{0,av}(t)$	Average system availability in (0,t)

Quantitative evaluation of the fault tree:
Reliability data for the input events

Category of failure data	Event	Reliability parameter	$q_i(t)$ =
Frequency	Event with no duration	$f =$ Frequency (Expected number of occurrences per hour)	0
On demand Probability	Component not activated during normal operation	$q =$ Probability that the component is not able to perform its function upon request	q
Test interval	Periodically tested (immediately repaired if a failure is detected only during a test).	$t^* =$Test interval, $\tau =$ Repair time (To be specified in hours) and $\lambda =$ Failure rate (Expected number of failures per hour)	$\frac{\lambda t^*}{2} + \frac{\tau}{t^*}$
Repairable unit	Repaired when a failure occurs	τ and λ	$\frac{\lambda\tau}{1+\lambda\tau}\left(1 - e^{-\frac{(1+\lambda\tau)t}{\tau}}\right) = \frac{MTTR}{MTTR + MTTF}$
Non repairable unit	Not repaired when a failure occurs	λ	$1 - e^{-\lambda t}$

For a repairable unit, $q_i(t)$ the probability that the unit cannot fulfill its function at time t.

Let construct the 2-state transition diagram, the transition rate matrix M and solve the system of the Chapman-Kolmogorov equations:

$$\frac{d}{dt}P(t) = P(t) \cdot M$$

Where $P(t) = [P_0(t), P_1(t)]$ is the state probability vector when the unit is ok at time $t = 0$.

We have, if λ_i is a constant failure rate and μ_i the constant repair rate:

$$P_0(t) = \frac{\lambda_i}{\lambda_i + \mu_i}\left(1 - e^{-(\lambda_i+\mu_i)t}\right) = q_i(t)$$

Probability that the TOP event occurs at time t

Properties:

- Uniquely determined by the $q_i(t)$'s
- If all failure data are in the category *on demand probability*, $Q_0(t) = Q_0$
- If at least 1 component in each minimal cut set is in *repairable or non-repairable unit*, $Q_0(t)$ increases in t
- If all failure data are in the category *frequency*, $Q_0(t) = 0$

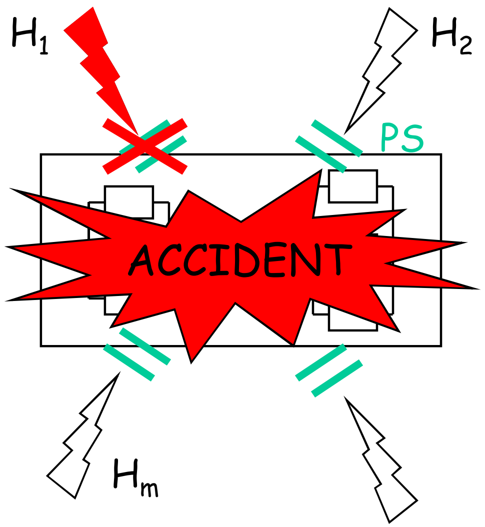
Upper Bound Approximation Method:

No Common Cause Failure

- Determination of all the minimal cut sets K_j
- Evaluation of each $\breve{Q}_j(t) = \prod_{i \in K_j} q_i(t)$ (independence of all input events)
- If ~~all the K_j are disjoint~~, we have $Q_0(t) \neq 1 - \prod_j (1 - \breve{Q}_j(t))$ → Upper Bound

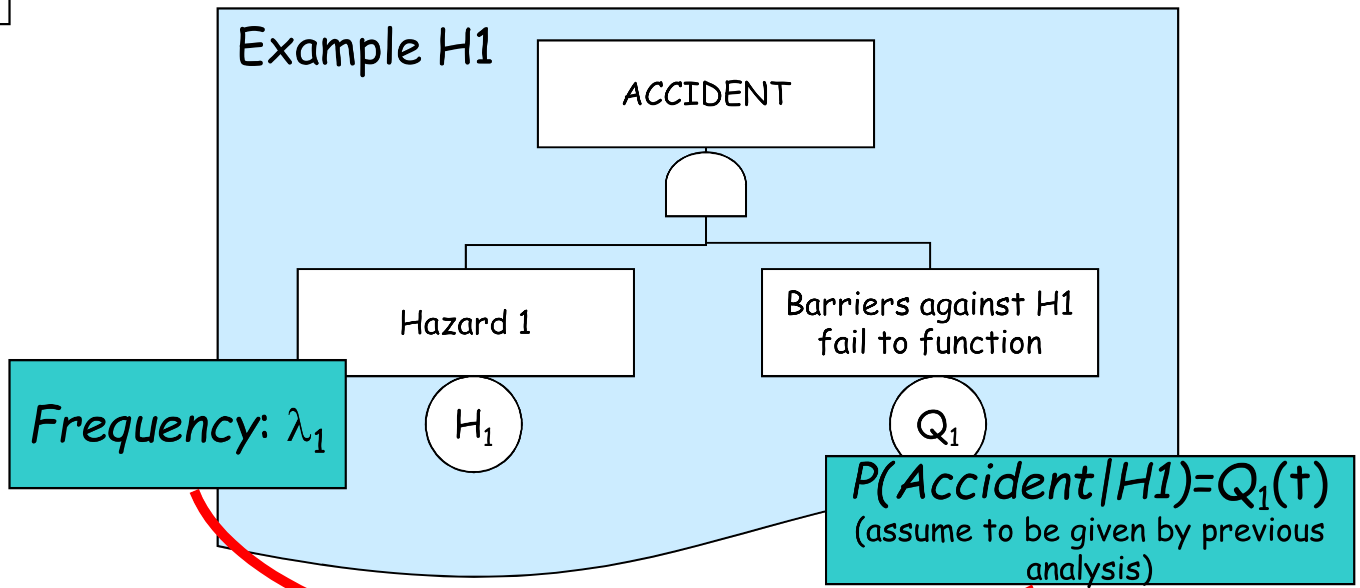
Good approximation if $q_i(t) \approx 0$

TOP Event Frequency



- The system is exposed to a set of Hazards $H_1, H_2, \ldots, H_m$
- The hazards are identified during system design

➔ Barriers and Protective Systems (PS)



Expected Frequency of TOP event

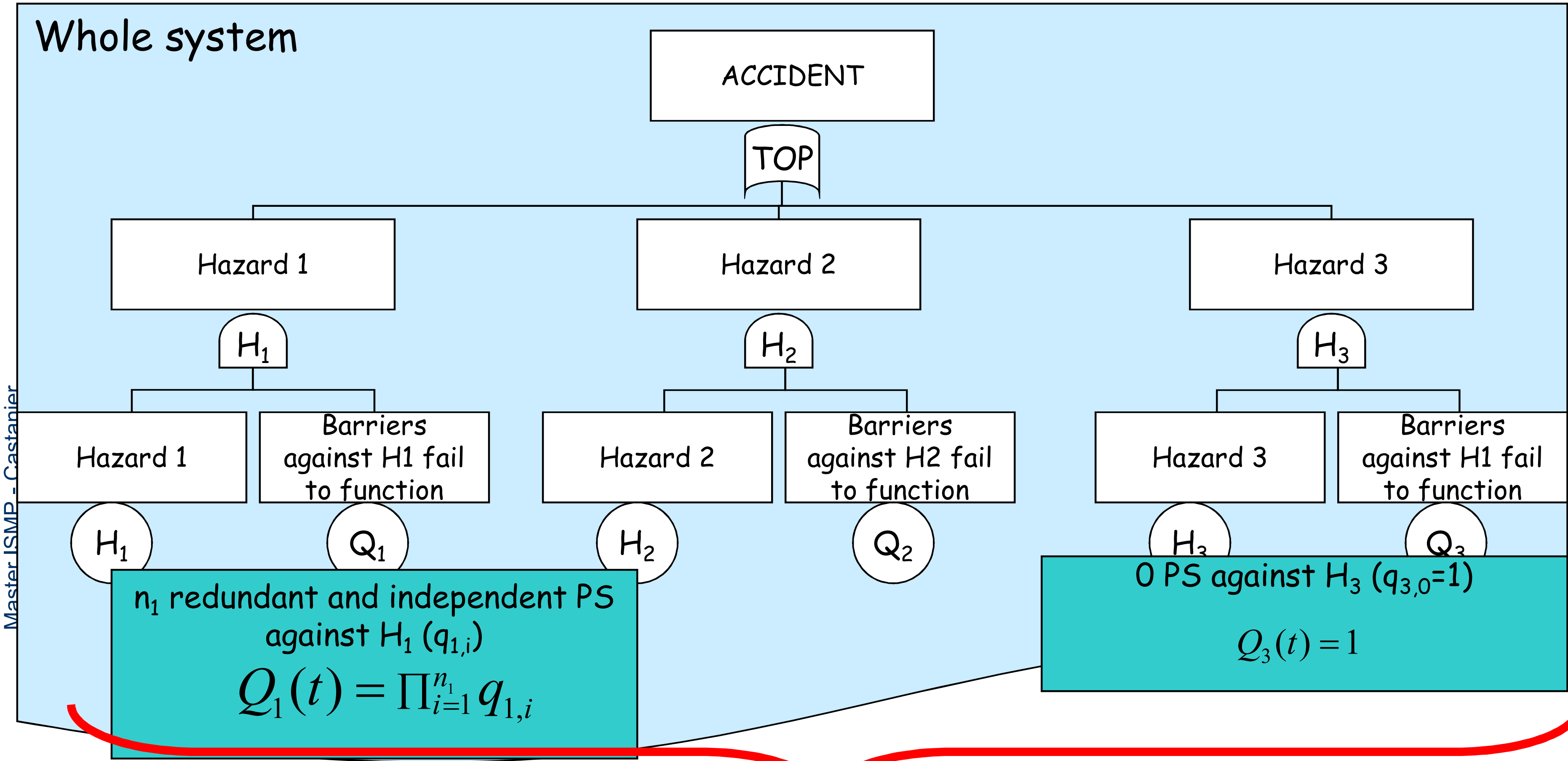
$\lambda_1 Q_1(t)$

Let N(t) denote the number of H1 in the time interval (0,t], and NA1(t) denote the number of A1 in the same interval.

When N(t)=n, NA1(t) will have a binomial distribution, i.e.

$$\Pr(NA_1(t) = m|N(t) = n) = C_n^m (Q_1(t))^m \left(1 - Q_1(t)\right)^{n-m}$$

Hence, the marginal distribution of NA1(t) is a Poisson with intensity (=frequency) $\lambda_1 Q_1(t)$.



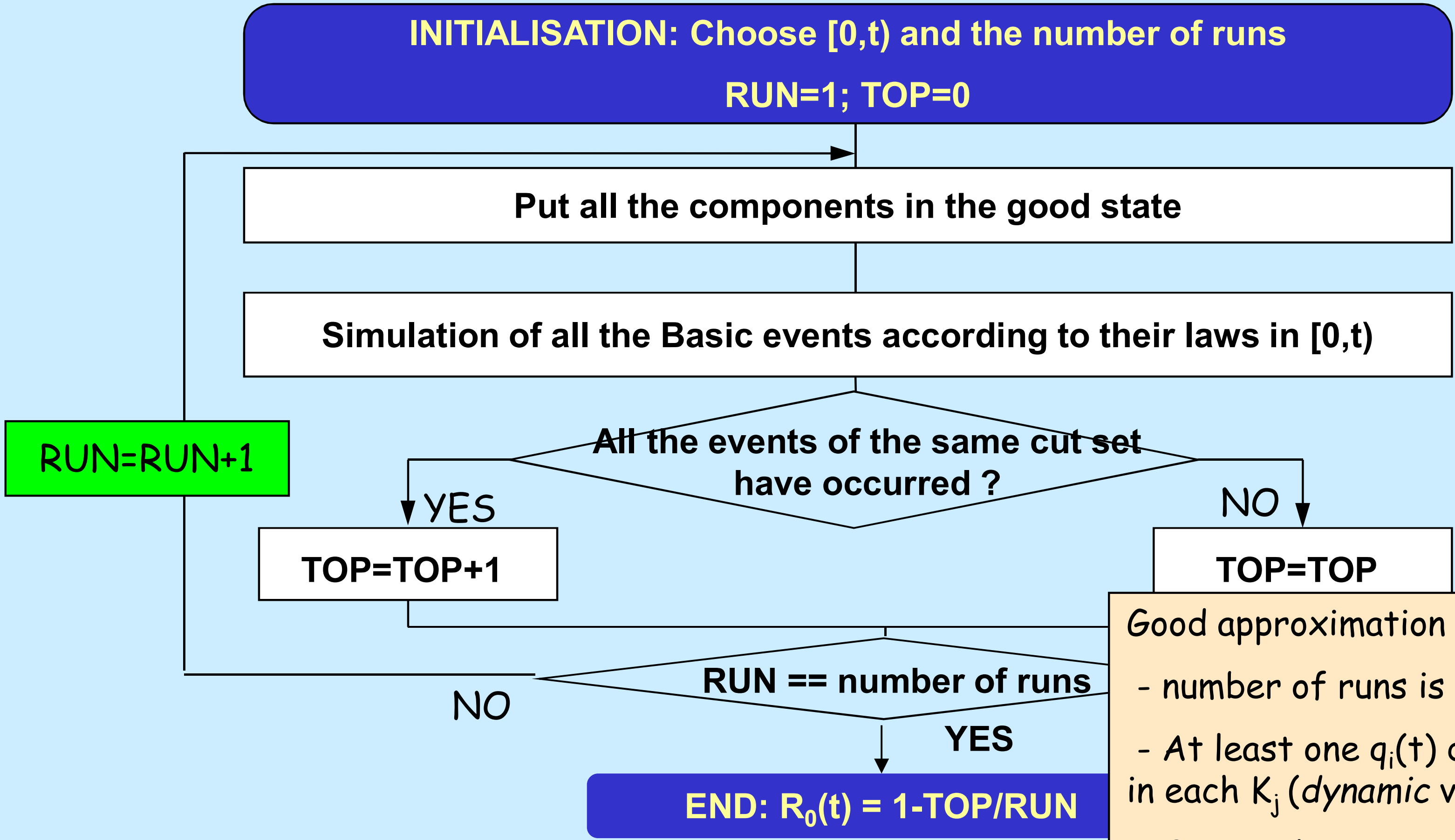
$$\lambda_{TOP} = \sum_{j=1}^{m} \lambda_j Q_j(t)$$

$$Freq(TOP) \approx \sum_{all\ cut\ sets\ K_j} \left\{ \sum_{i \in K_j} \lambda_i \prod_{l \in K_j, l \neq i} q_l(t) \right\}$$

Calculation Using Simulation

The Reliability function $R_0(t)$=P(«TOP event has not occurred in [0,t)») where the system is assumed to be perfect at t=0.

Monte-Carlo Simulation



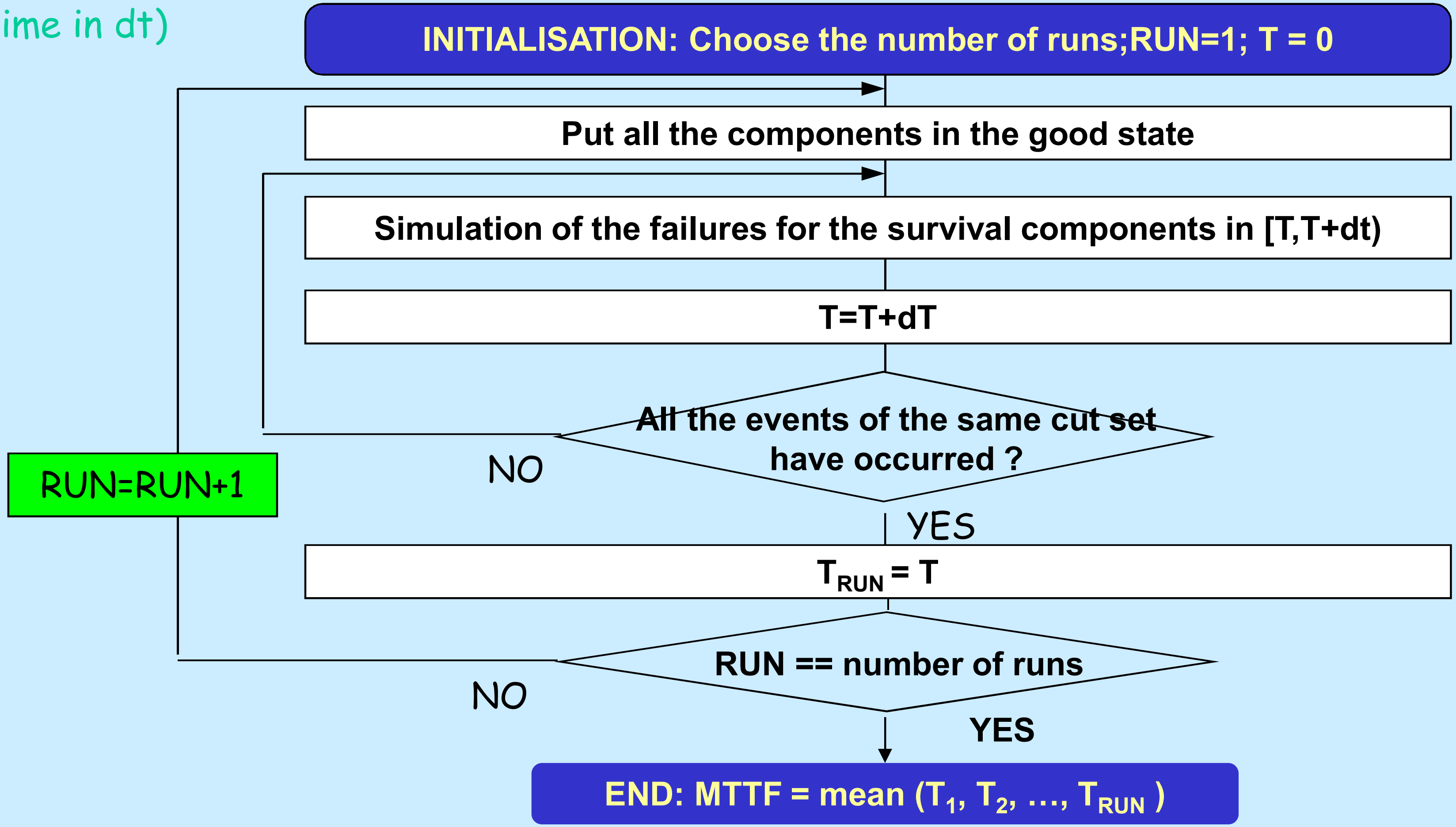
Good approximation if:

- number of runs is large
- At least one $q_i(t)$ depending of t in each K_j (*dynamic* vs *static* tree)
- System is not very reliable

The MTTF is the Mean Time to First Failure, ie. when the time of the failure when the system is assumed to be «as good as new» at t=0.

Monte-Carlo Simulation

(discretization of the time in dt)



The Inclusion-Exclusion Principle:

$$P\left(\bigcup_{j=1}^{k} E_j\right) = \sum_{j=1}^{k} P(E_j) - \sum_{i<j} P(E_i \cap E_j) + \ldots + (-1)^{k+1} P\left(\bigcap_{j=1}^{k} E_j\right)$$

- where Ej = event that the components of Kj are all failed.

Structure function method

Pivotal Decomposition, ….

Advantage

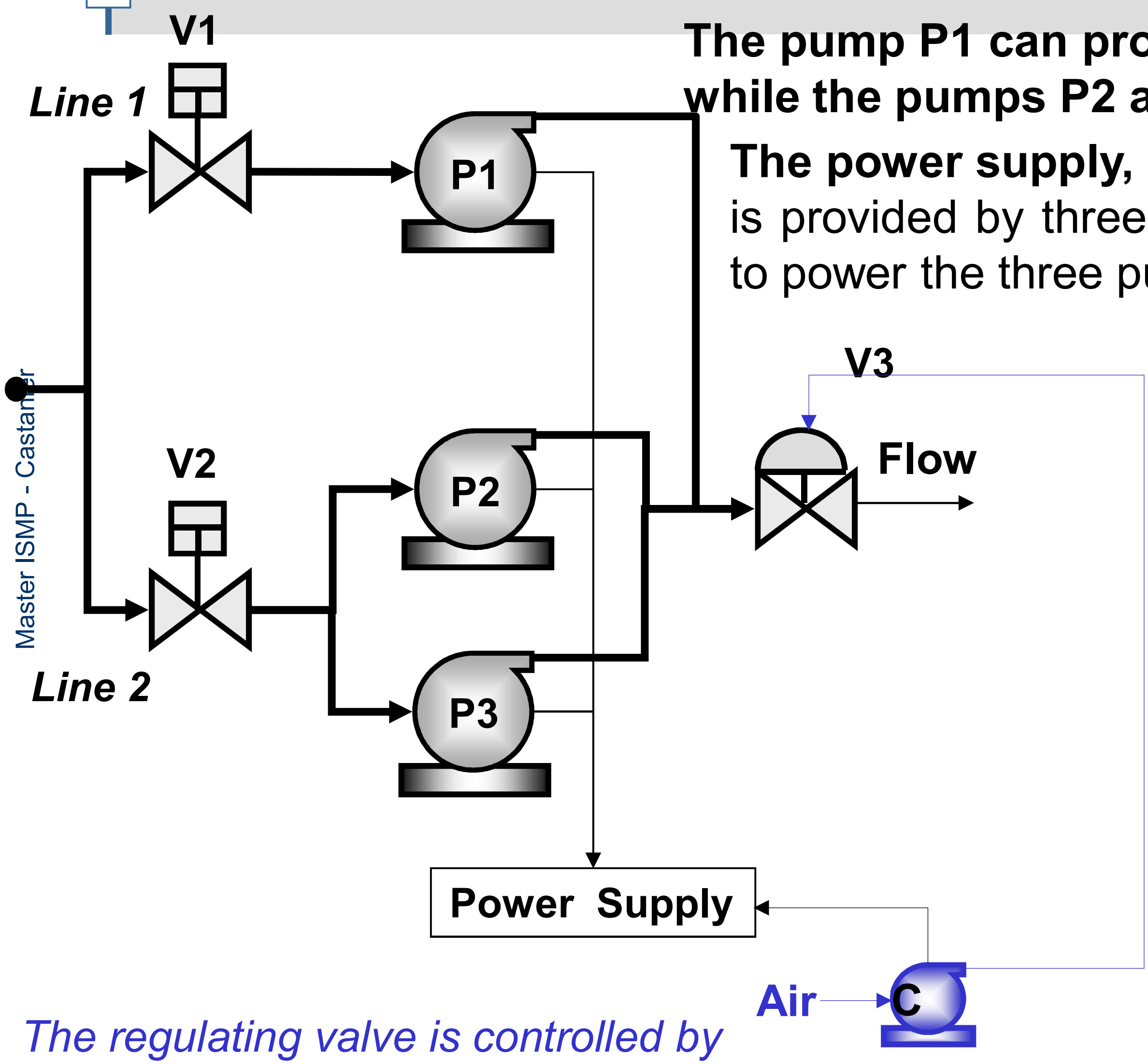
- Method for quantitative and qualitative analysis
- Very easy to modelize and to implement
- Possibility to take into account many types of events
- Evaluation of the common cause failures
- Support for the allocation of the objectives (Seveso II)

Limitations of the method

- The results obtained with this method can be (completely) inaccurate:
  - for the analyse of a complex systems with interactive elementary components.
  - for the analyse of multiphase systems (the mission of the system can be divided in many consecutive time periods)
  - for the analyse of events that are time-dependent

when the Basic events are non-independent

Fault tree: Exercice 1



The pump P1 can provide 100% of the required flow, while the pumps P2 and P3 only provide 50% each.

The power supply, common to these three pumps, is provided by three lines, two of which are sufficient to power the three pumps.

A **fourth line** serves to **supply the compressor**.

In normal operation, the three pumps operate simultaneously and the flow is distributed in both lines. It is assumed that the upstream flow can always be assured.

the undesirable event is defined as follows:

"Flow rate less than required flow"

The regulating valve is controlled by compressed air (compressor). It closes due to lack of air

Items	λ
Compressor	1e-5
Electrical contactors	1e-5
Voting system 2/3 (électrique)	1e-6
Electrical lines	1e-7
Pump 1	2e-4
Pumps 2 & 3	1e-4
Valves 1 & 2	2e-6
Regulating Valve 3	5e-6

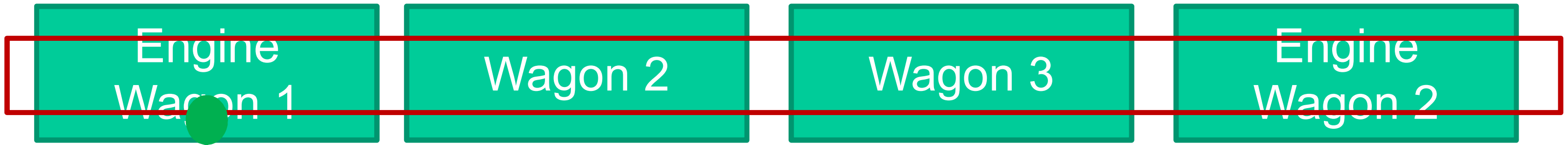
Describe the pumping system through:

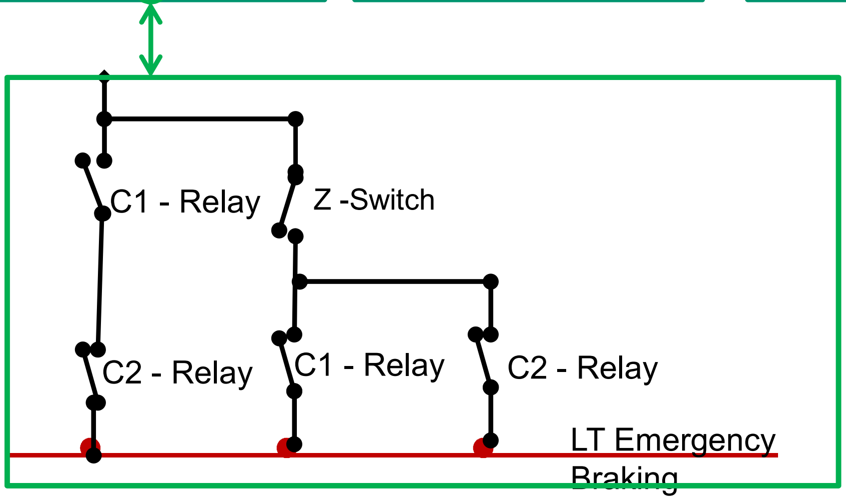
- its minimal cut sets
- its different reliability metrics (Reliability, Availability, …)

Fault tree: Exercice 2

Emergency Train Brake (EB)

- Activation if « non power supply of the line EB »





Mode 1 Reliability
$$\begin{cases} \lambda_{C1} = 1.28e-7\ h^{-1} \\ \lambda_{C2} = 1.28e-7\ h^{-1} \\ \lambda_{Z} = 6.82e-9\ h^{-1} \end{cases}$$

Mode 2 Safety
$$\begin{cases} \lambda_{C1} = 2.21e-5\ h^{-1} \\ \lambda_{C2} = 2.21e-6\ h^{-1} \\ \lambda_{Z} = 5.82e-7\ h^{-1} \end{cases}$$

Analyze the ETB from a reliability and safety perspectives

Reliability perspective:

- Definition of the ERF = « no power of the train line EB »
- Definition of the initial conditions (relays are closed, the switch is open and power supply in the unit)
- Be aware of the reliability assessment in case of a passive redundancy

Safety perspective:

- Definition of the ERS = « no shutdown of the supply in the train line EB on demand »
- Definition of the initial conditions (no supply in the line)
- Integration of the common cause failures on the relays?
- Integration of testing interval on the components…