

# Young Researchers Seminar 2009

Torino, Italy, 3 to 5 June 2009

## Optimal design of automated dependable system architectures

Application to a railroad transportation system

CLARHAUT Joffrey



# Railroad system

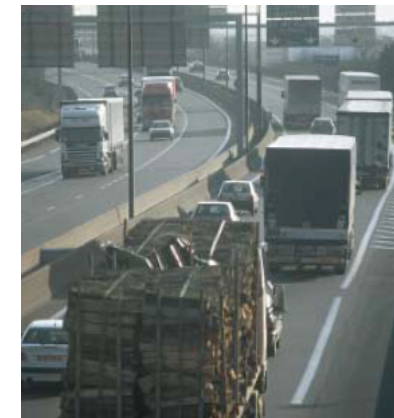
Railroad vehicle transportation system

=

Trucks on trains



- Advantages:
  - Decreasing congestion of roads
  - Less pollution and consumption
  - ...
- Need of dependability improvements:
  - Contributing to availability
  - Increasing of system's safety



Optimal design of automated dependable system

CLARHAUT Joffrey



# Concept of the smart wagon

**Smart sensors integers functions like:**

- monitoring,
- supervising,
- control,
- ...

---

Optimal design of automated dependable system

CLARHAUT Joffrey



# Concept of the smart wagon

**Smart sensors integers functions like:**

- monitoring,
- supervising,
- control,
- ...

**Smart wagon**

=

**instrumented wagon (sensors, actuators, ...) with the same functions of the smart sensor**

**Why a smart wagon ?**

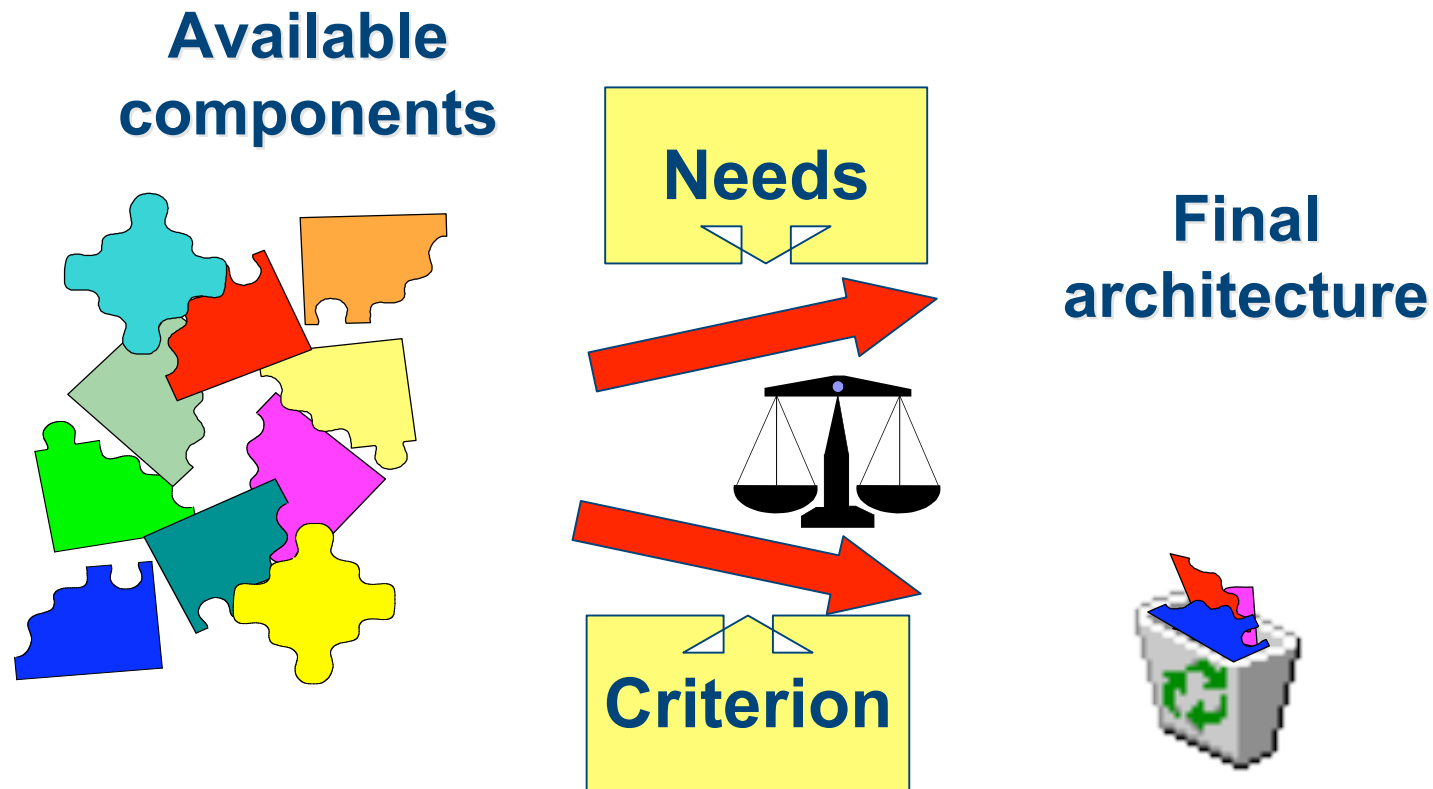
- Link with other system's parts
- Present in all system's operational phases

# Content

- Needs of a design methodology of automated systems
  - General concepts
  - Cuts and scenarii
  - Formalizations
- Presentation of the proposed design methodology
  - Modeling step
  - Optimization step
  - Case study
- Results
  - Comparison with traditional fault trees
  - Interest of scenarii
- Conclusion and future works

# Designing a dependable system

Find a feasible architecture that guarantees an acceptable level of dependability



Optimal design of automated dependable system

CLARHAUT Joffrey



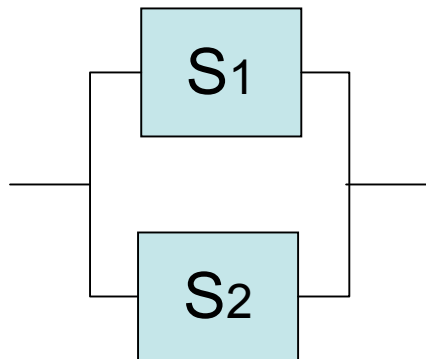
# System's dependability level evaluation using scenarii

## Cut:

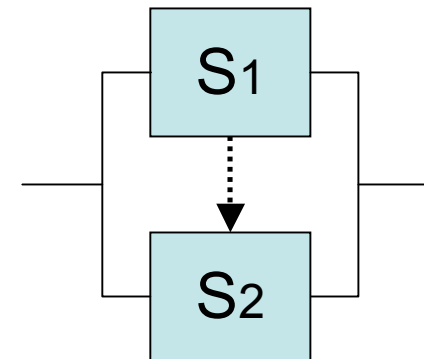
sequence of failures that leads the system to a precise dreaded event

System S with two components

Active redundancy



Passive redundancy



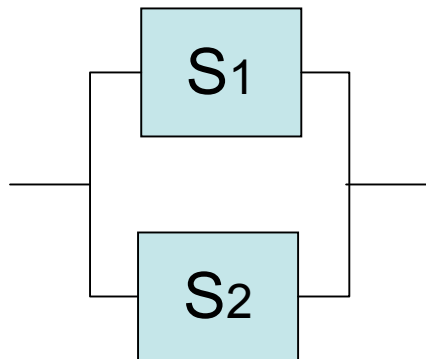
# System's dependability level evaluation using scenarii

## Cut:

sequence of failures that leads the system to a precise dreaded event

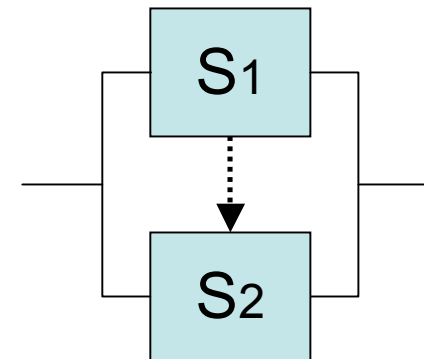
System S with two components

Active redundancy



System fails if  
{ S1 fails, S2 fails }

Passive redundancy

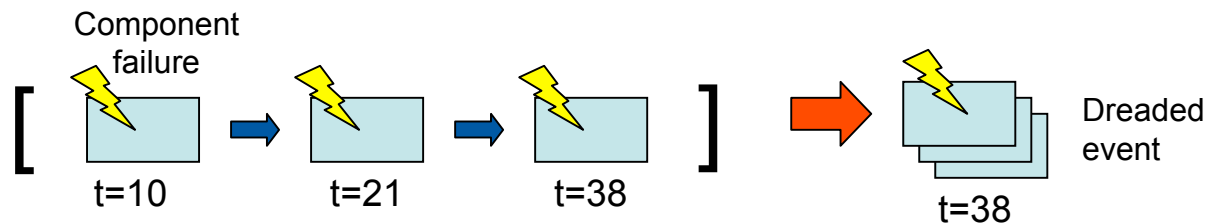


System fails if  
{ S1 fails, S2 fails }

# System's dependability level evaluation using scenarios

## Scenario:

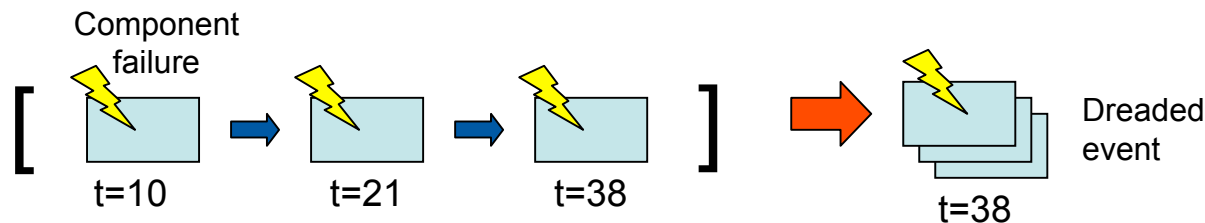
time ordered sequence of failures that leads the system to a precise dreaded event



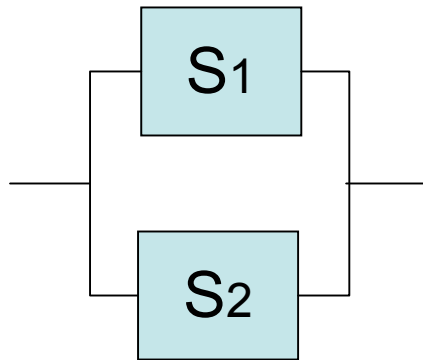
# System's dependability level evaluation using scenarios

## Scenario:

time ordered sequence of failures that leads the system to a precise dreaded event



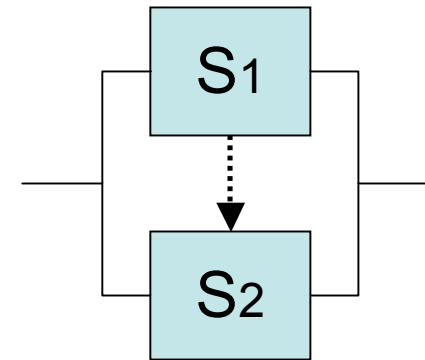
### Active redundancy



System fails if

[ S1 fails, S2 fails ] or [ S2 fails, S1 fails ]

### Passive redundancy



System fails if

[ S1 fails **then** S2 fails ]

Optimal design of automated dependable system

CLARHAUT Joffrey



# Formalizations (1)

- A **scenario** ( $\Psi_D$ ) is a time ordered sequence of  $n$  failures that leads the system to a precise dreaded event ( $D$ )

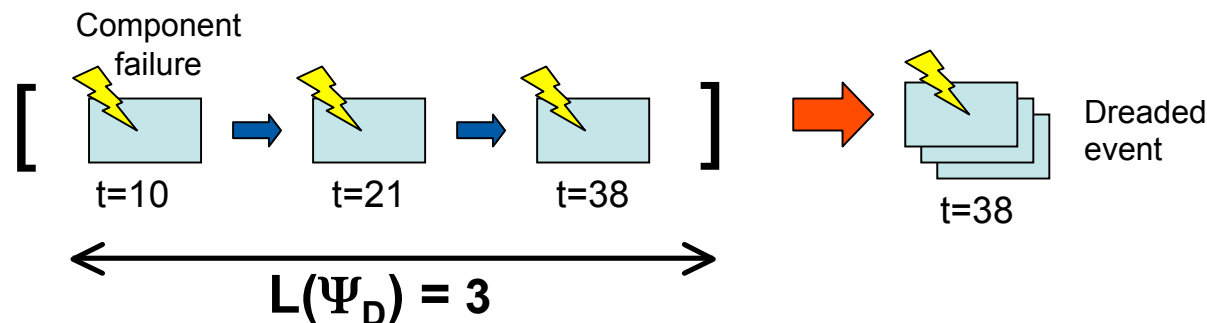
$$\Psi_D = [F_i^1, \dots, F_j^n]$$

- A **set** of  $m$  scenarii is denoted :

$$\Phi_D = \{ \Psi_D^1, \dots, \Psi_D^i, \dots, \Psi_D^m \}$$

- The **length** of a scenario from this set is denoted :

$$L(\Psi_D) = \text{card}(\Psi_D^i)$$



## Formalizations (2)

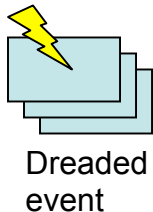
- The **minimal length** of a set of scenarii ( $\Phi_D$ ) is denoted :

$$L_{\min}^D = \min_{1 \leq i \leq m} L(\Psi_D^i)$$

- The **number of scenarii** with minimal length is denoted :

$$N_{\min}^D = \text{card}(\Delta_D) \text{ with } \Delta_D \subset \Phi_D$$

**Dreaded event:**



Characterized by: - the minimal length ( $L_{\min}^D$ ) of scenarii  
- the number ( $N_{\min}^D$ )

**Link with dependability:**

Dependability level  
( $DL^S$ )



if



-  $L_{\min}^D$



-  $N_{\min}^D$

Optimal design of automated dependable system

CLARHAUT Joffrey



# Design of a dependable automated system

Design methodology:

- Modeling step
- Optimization step

---

Optimal design of automated dependable system

CLARHAUT Joffrey



# Design of a dependable automated system

Available components  
(sensors, actuators, ...)

Component  
organizations

Design methodology:  
- Modeling step  
- Optimization step

Set of optimal  
equipment  
architectures

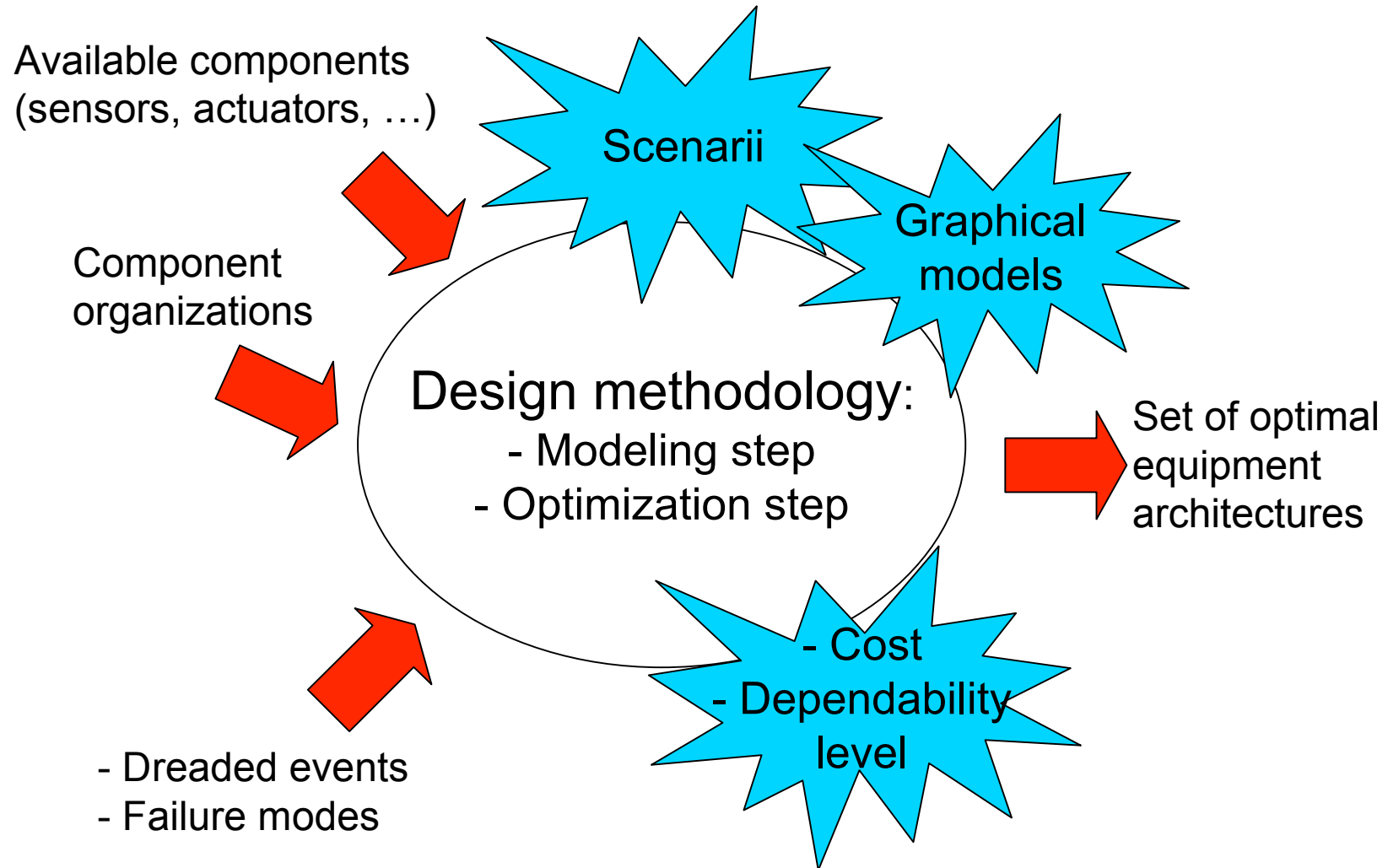
- Dreaded events
- Failure modes

Optimal design of automated dependable system

CLARHAUT Joffrey



# Design of a dependable automated system



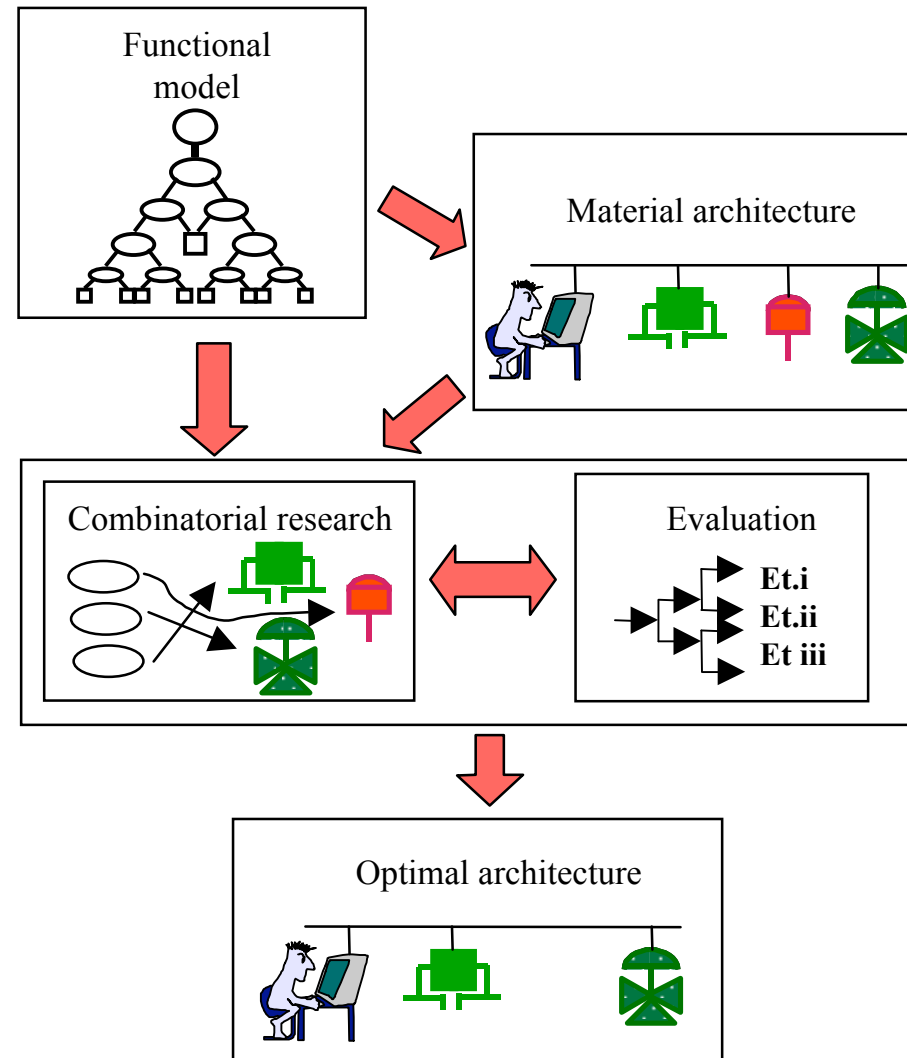
# Design of a dependable automated system

## - Methodology :

- 1) Functional model
- 2) Material architecture
- 3) Combinatorial research + Evaluation

## - Final result :

Set of optimal architectures



Optimal design of automated dependable system

CLARHAUT Joffrey



# Case study

Design of a fire protection system for the smart wagon

- **Two missions:**
  - Detect a fire
  - Send an alarm to operators (train driver, ...).
- **Two dreaded events :**
  - No fire alarm when a fire is present (ER1).
  - False alarm (fire alarm without fire, ER2).

➔ Evaluate a level of dependability and a financial cost

# Definition of basic components

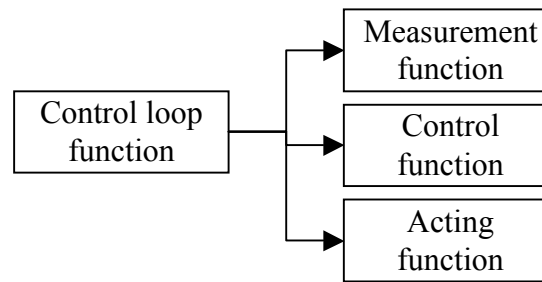
Basic component	Failure modes	Cost	Component possible organisations
Power supply	- Unexpected stop	5	- single component - 2 components in active redundancy - 2 components in passive redundancy
PLC	- Unexpected stop with alarm - Unexpected stop without alarm	3	- single component - 2 components with alarm priority - 2 components without alarm priority
Heat detector	- Continuously active - Continuously inactive	1	- single component - 2 components in serial - 2 components in parallel
Smoke detector	- Continuously active - Continuously inactive	1	- single component - 2 components in serial - 2 components in parallel

# Modeling step (1)

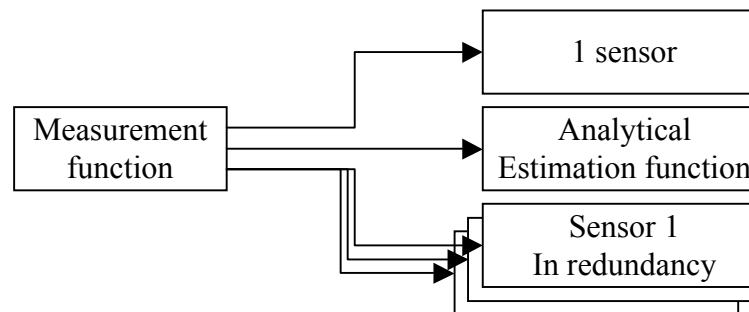
## Functional model:

System's hierarchical analysis represented by a tree with three types of nodes:

- Associative node:



- Alternative node:

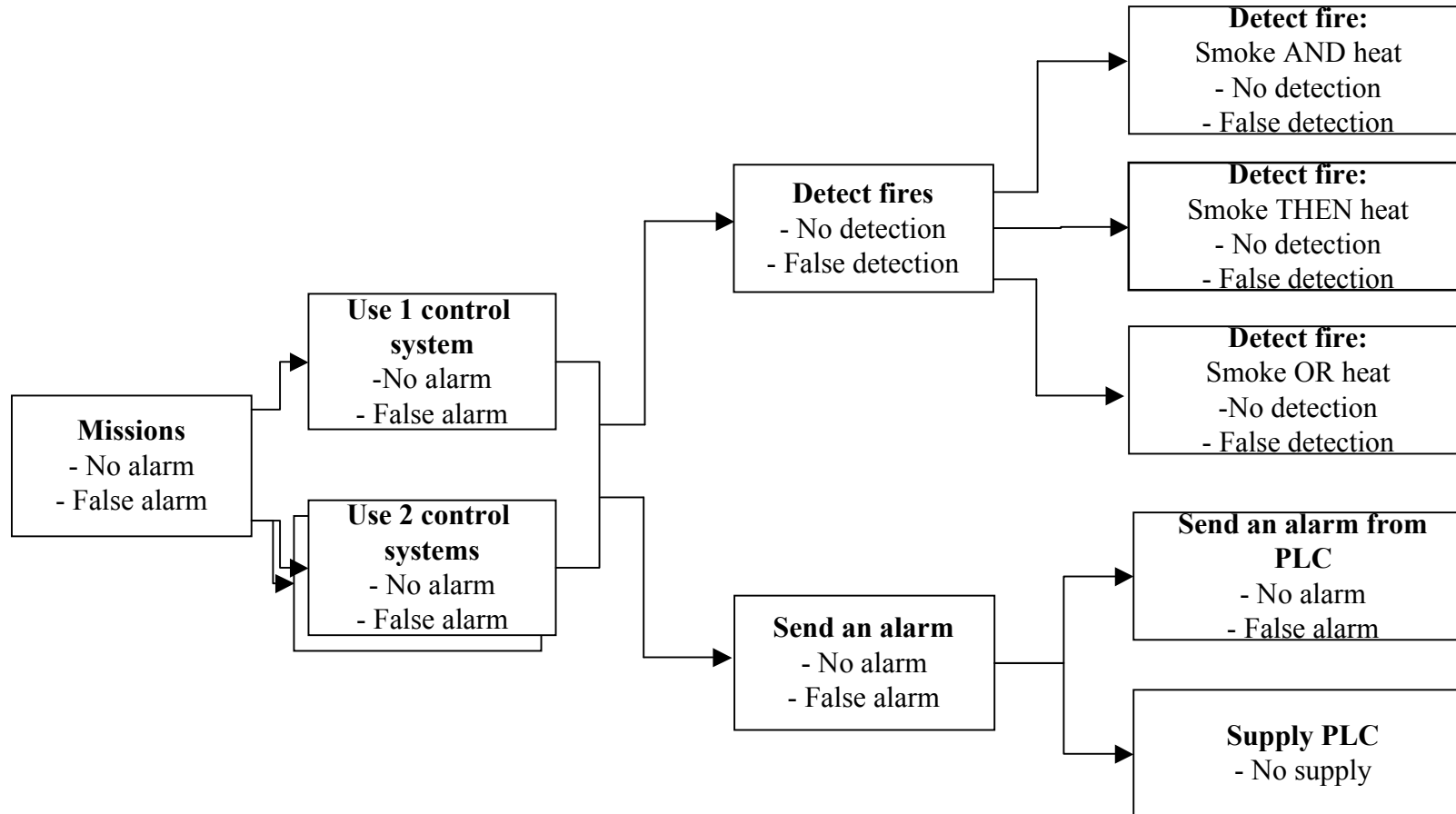


- Elementary node:



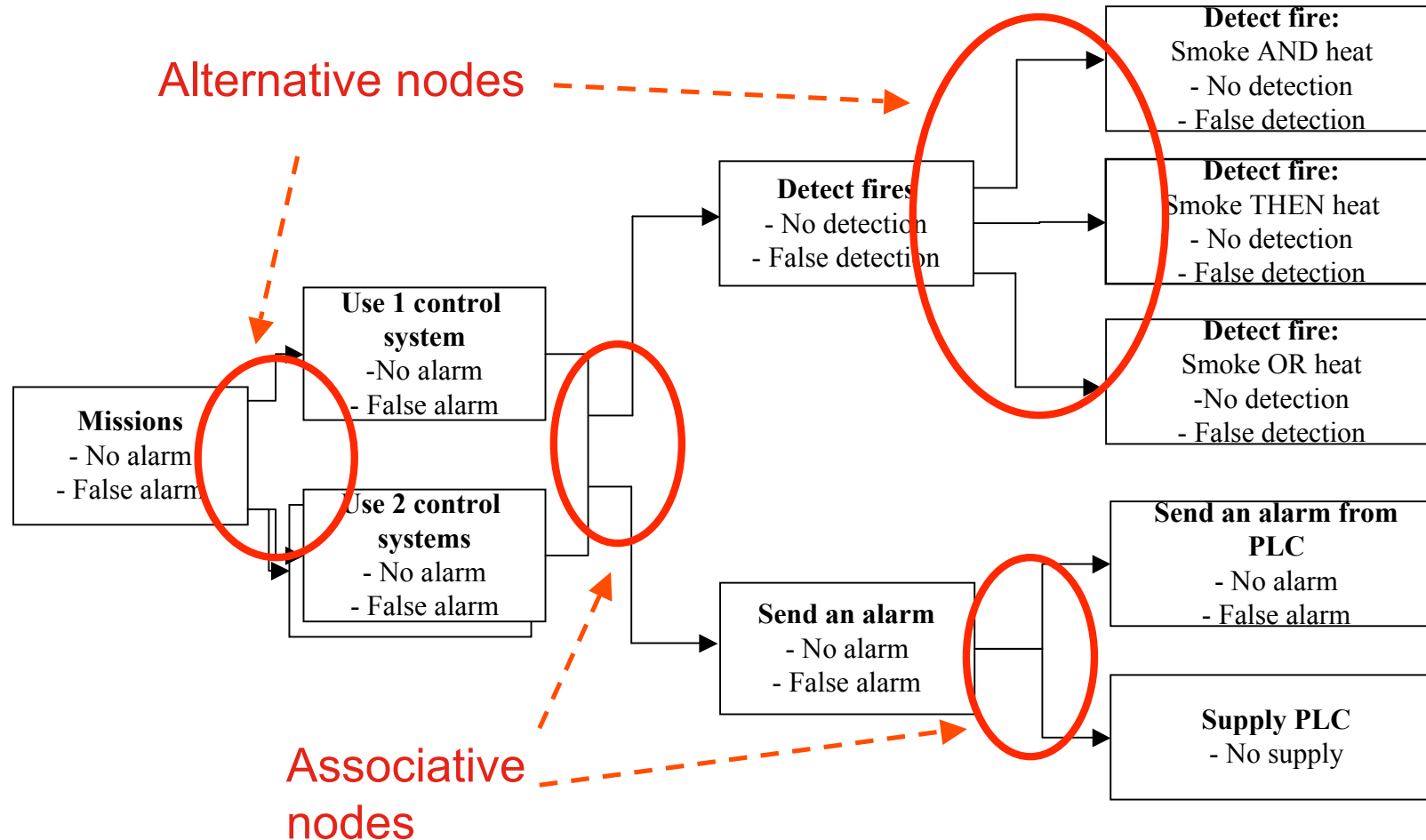
# Modeling step (2)

Fire protection system :



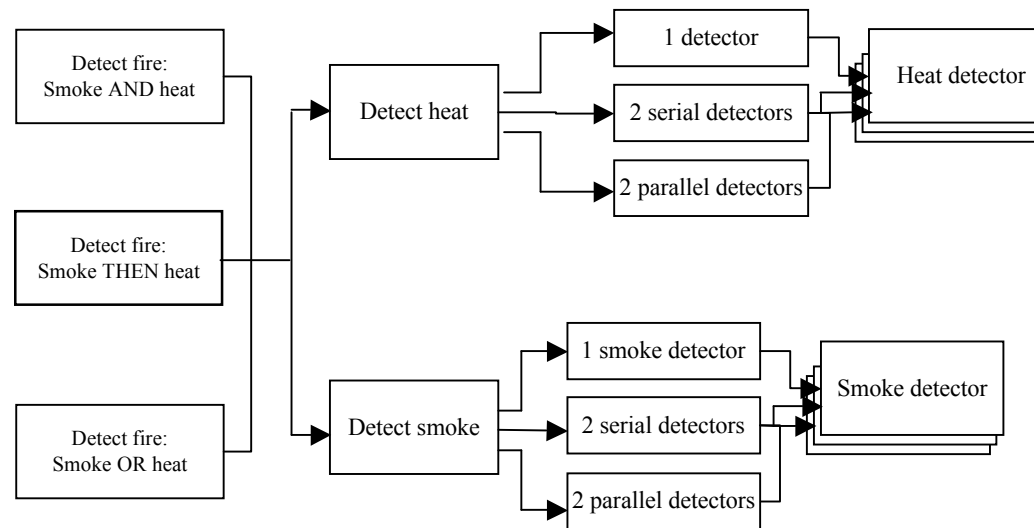
# Modeling step (2)

Fire protection system :



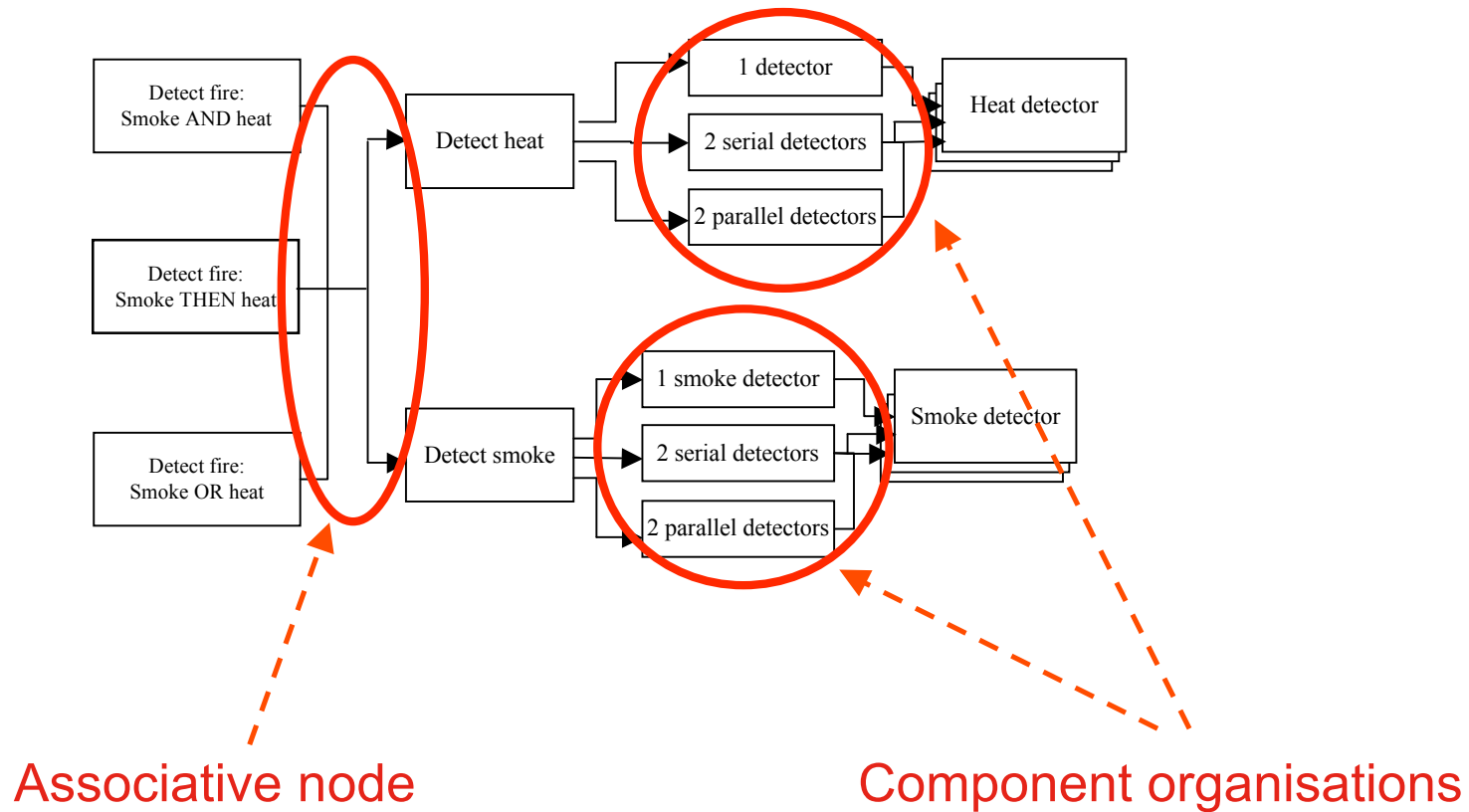
# Modeling step (3)

Functional model of the fire protection system:



# Modeling step (3)

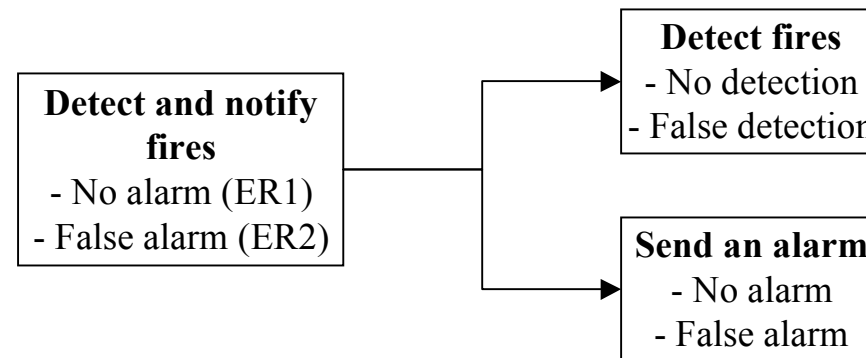
Functional model of the fire protection system:



# Modeling step (4)

## Improved multi-fault tree:

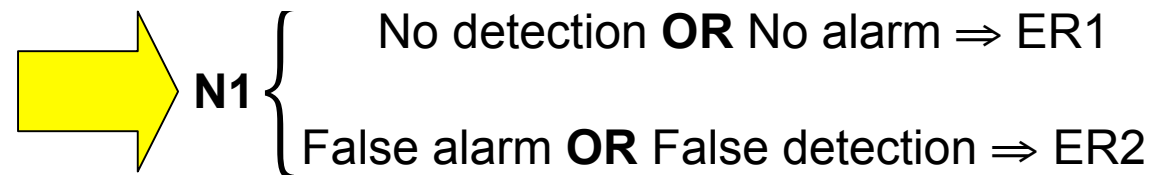
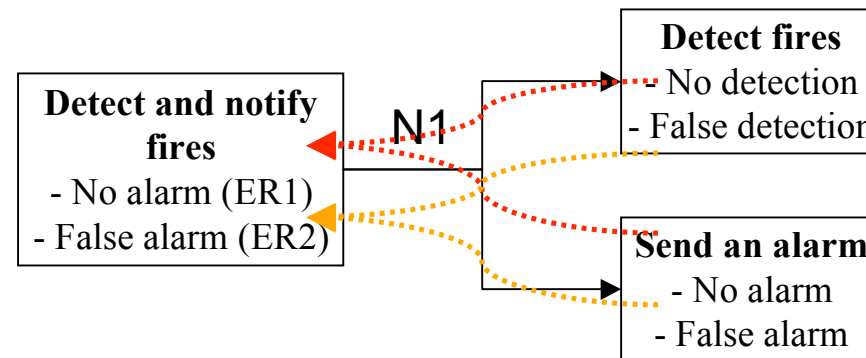
- Based on the previous functional model.
- Consists in associating to each node the set of failure modes that affect the accomplishment of the function.



# Modeling step (4)

## Improved multi-fault tree:

- Based on the previous functional model.
- Consists in associating to each node the set of failure modes that affect the accomplishment of the function.



# Modeling step (5)

## Missions of operators:

- Represent relations between different failures in the modeling step.
- Apply computational properties in the optimization step.

# Modeling step (5)

## Missions of operators:

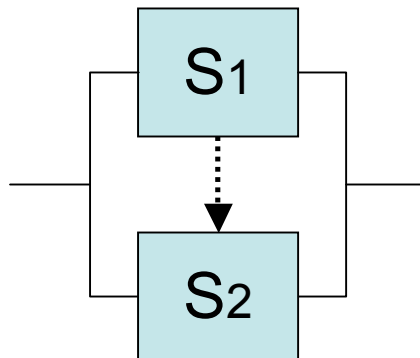
- Represent relations between different failures in the modeling step.
- Apply computational properties in the optimization step.

## Classical operators:

- AND
- OR

## Temporal operators:

- AND-Priority (PAND)
- Sequential (SEQ)



System fails  
if S1 fails  
then S2 fails

# Modeling step (5)

## Examples of computational properties:

- Let A, B and C, three dreaded events and  $\Delta_A$ ,  $\Delta_B$  and  $\Delta_C$  the three sets of minimal scenarios.
- C results from the association of A and B with one of the previous operators.

For C = A **AND** B:

$$L_{\min}^C = L_{\min}^A + L_{\min}^B$$
$$N_{\min}^C = \frac{(L_{\min}^A + L_{\min}^B)!}{L_{\min}^A! \times L_{\min}^B!} \times N_{\min}^A \times N_{\min}^B$$

For C = A **PAND** B:

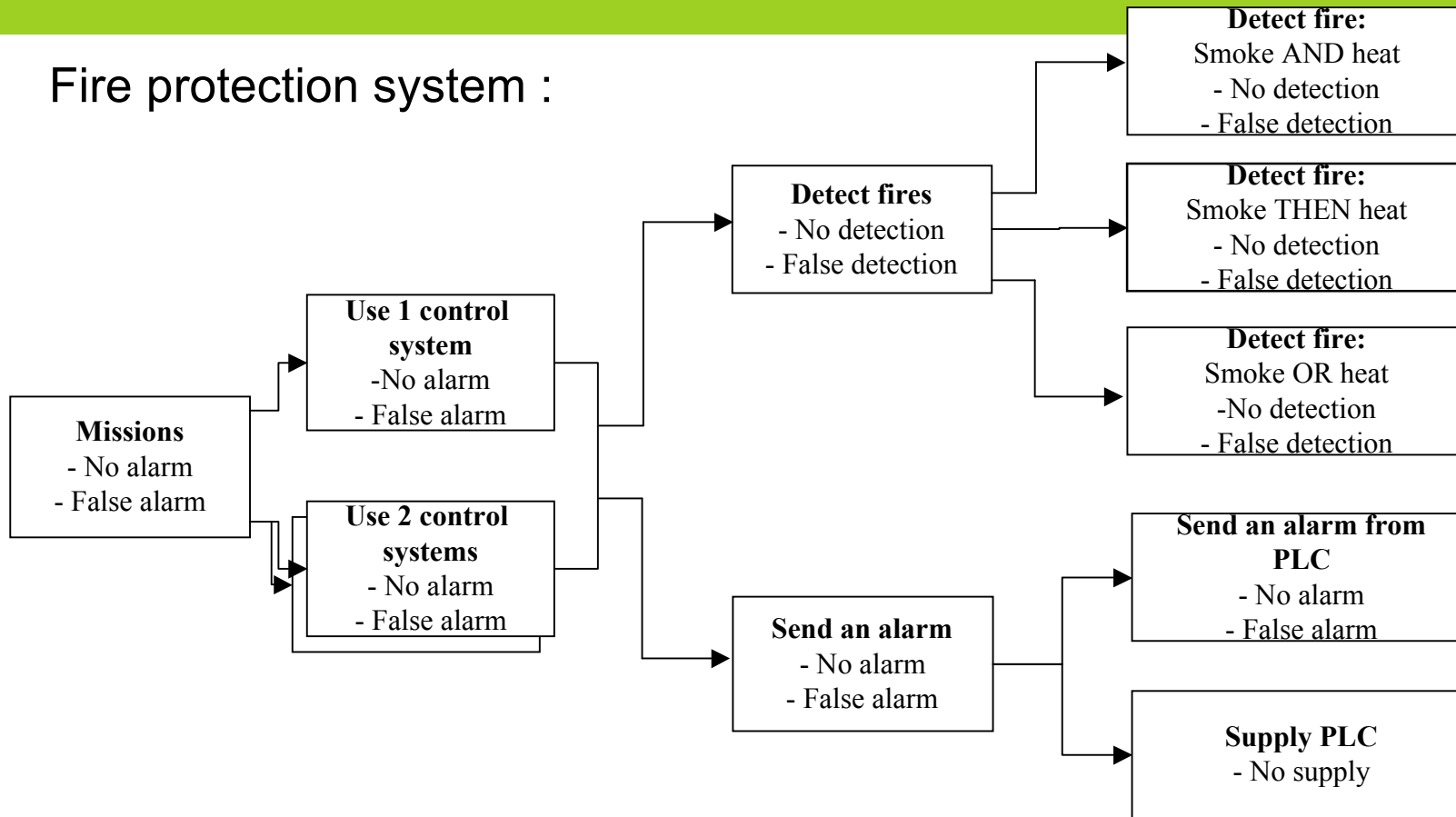
$$L_{\min}^C = L_{\min}^A + L_{\min}^B$$
$$N_{\min}^C = \frac{((L_{\min}^A - 1) + L_{\min}^B)!}{(L_{\min}^A - 1)! \times L_{\min}^B!} \times N_{\min}^A \times N_{\min}^B$$

For C = A **SEQ** B:

$$L_{\min}^C = L_{\min}^A + L_{\min}^B$$
$$N_{\min}^C = N_{\min}^A + N_{\min}^B$$

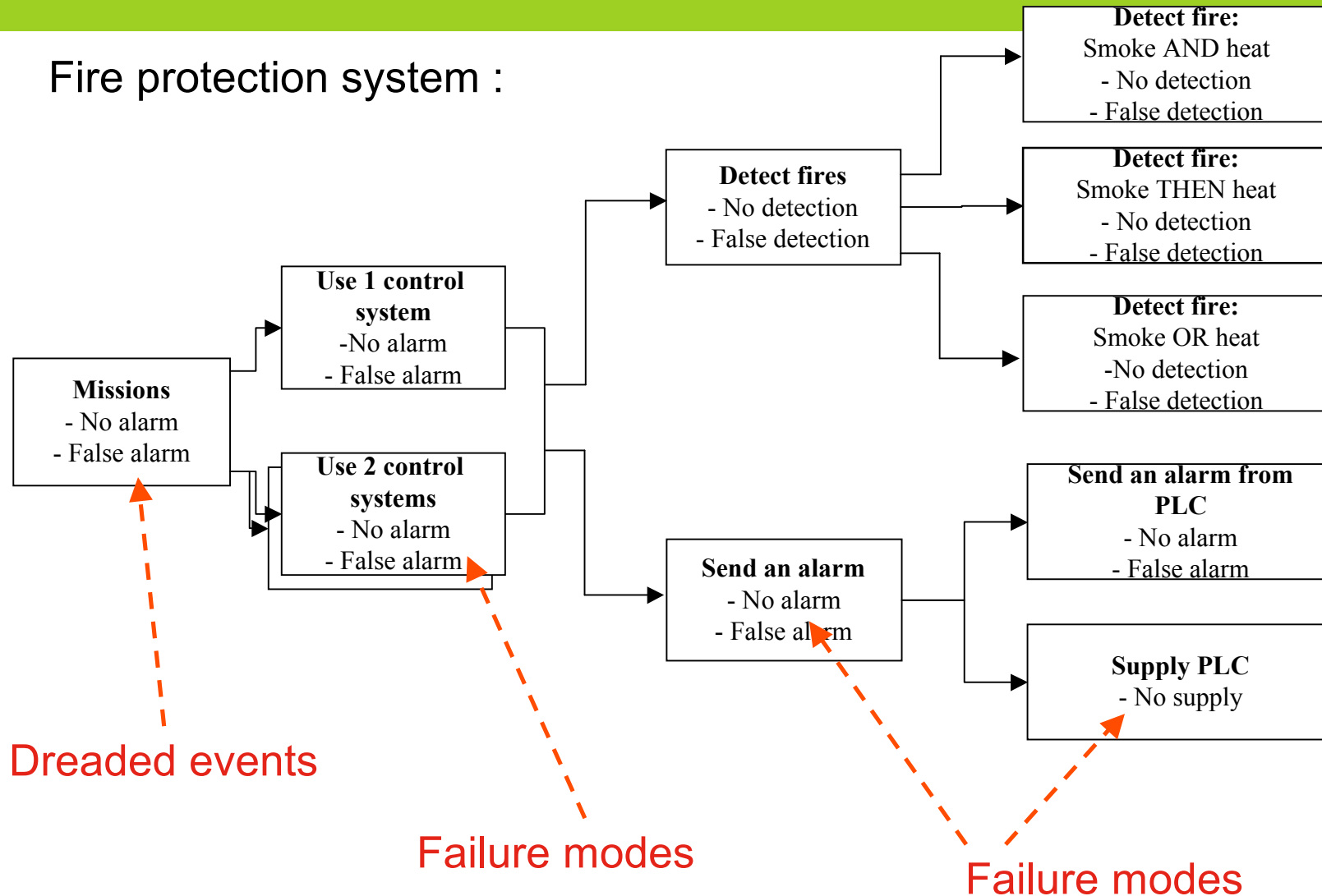
# Modeling step (6)

Fire protection system :



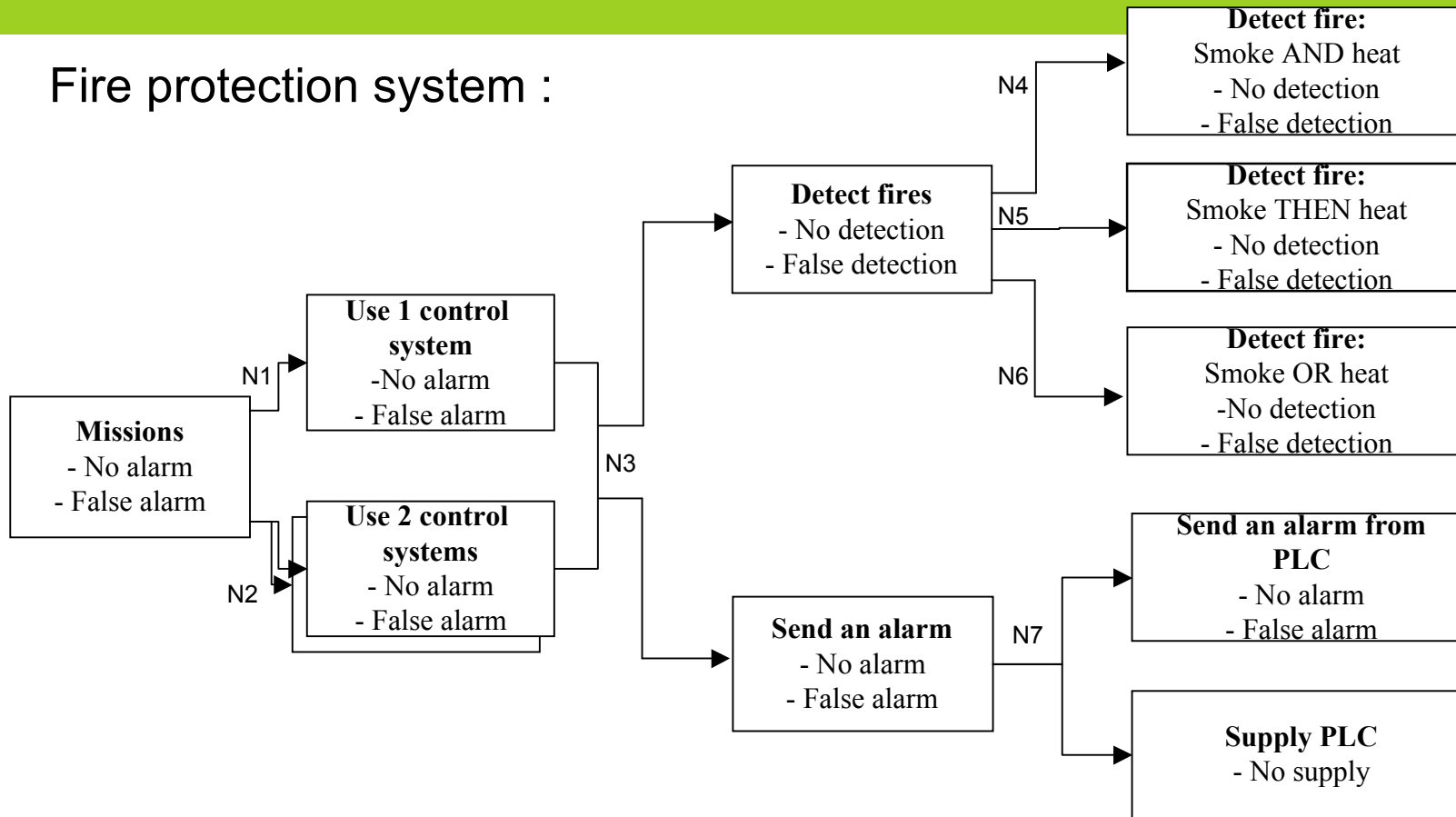
# Modeling step (6)

Fire protection system :



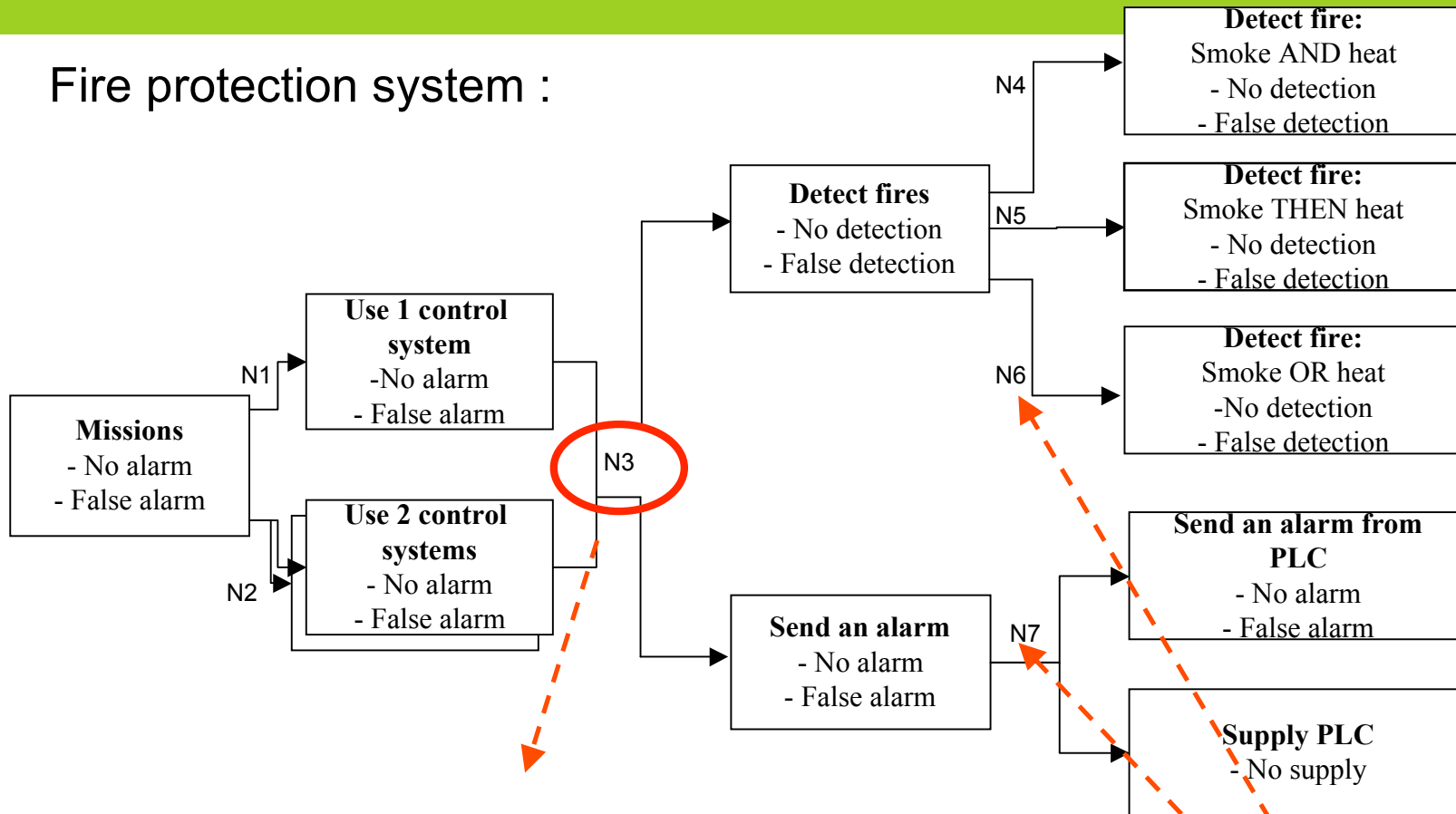
# Modeling step (7)

Fire protection system :



# Modeling step (7)

Fire protection system :

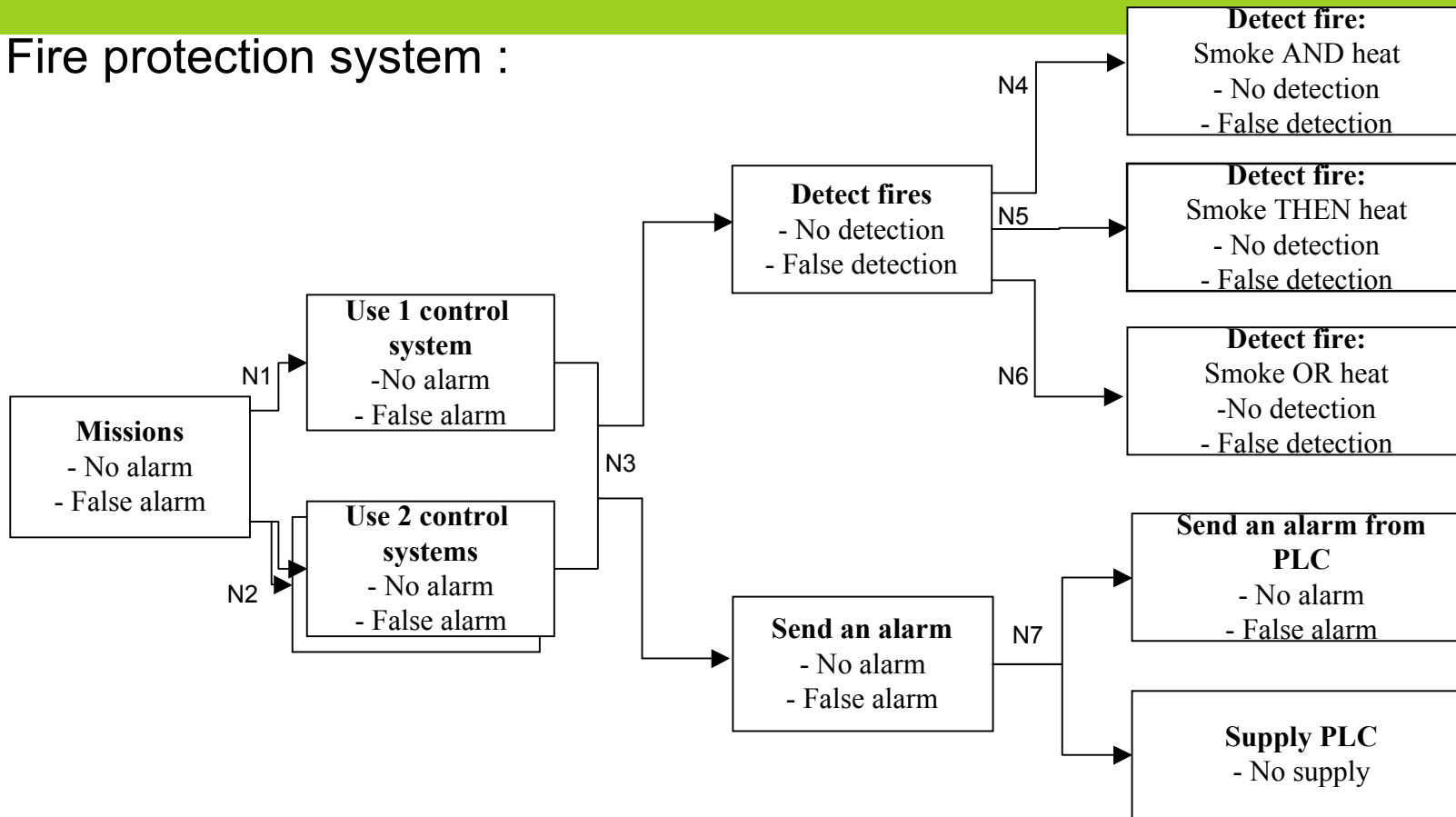


**N3** {
   
 No detection **OR** No alarm  $\Rightarrow$  ER1
   
 False alarm **OR** False detection  $\Rightarrow$  ER2

Failure relationships

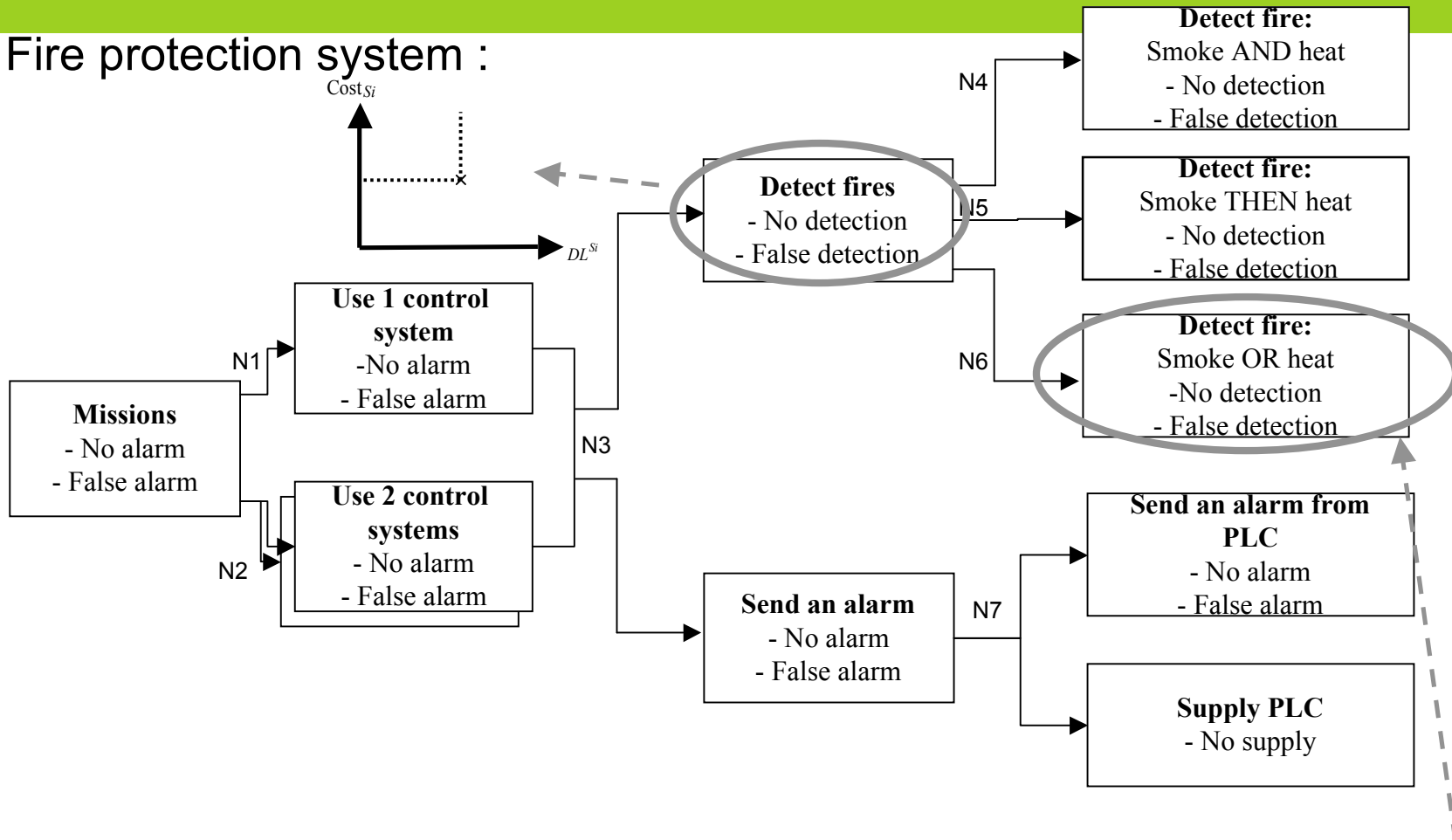
# Optimisation step

Fire protection system :



# Optimisation step

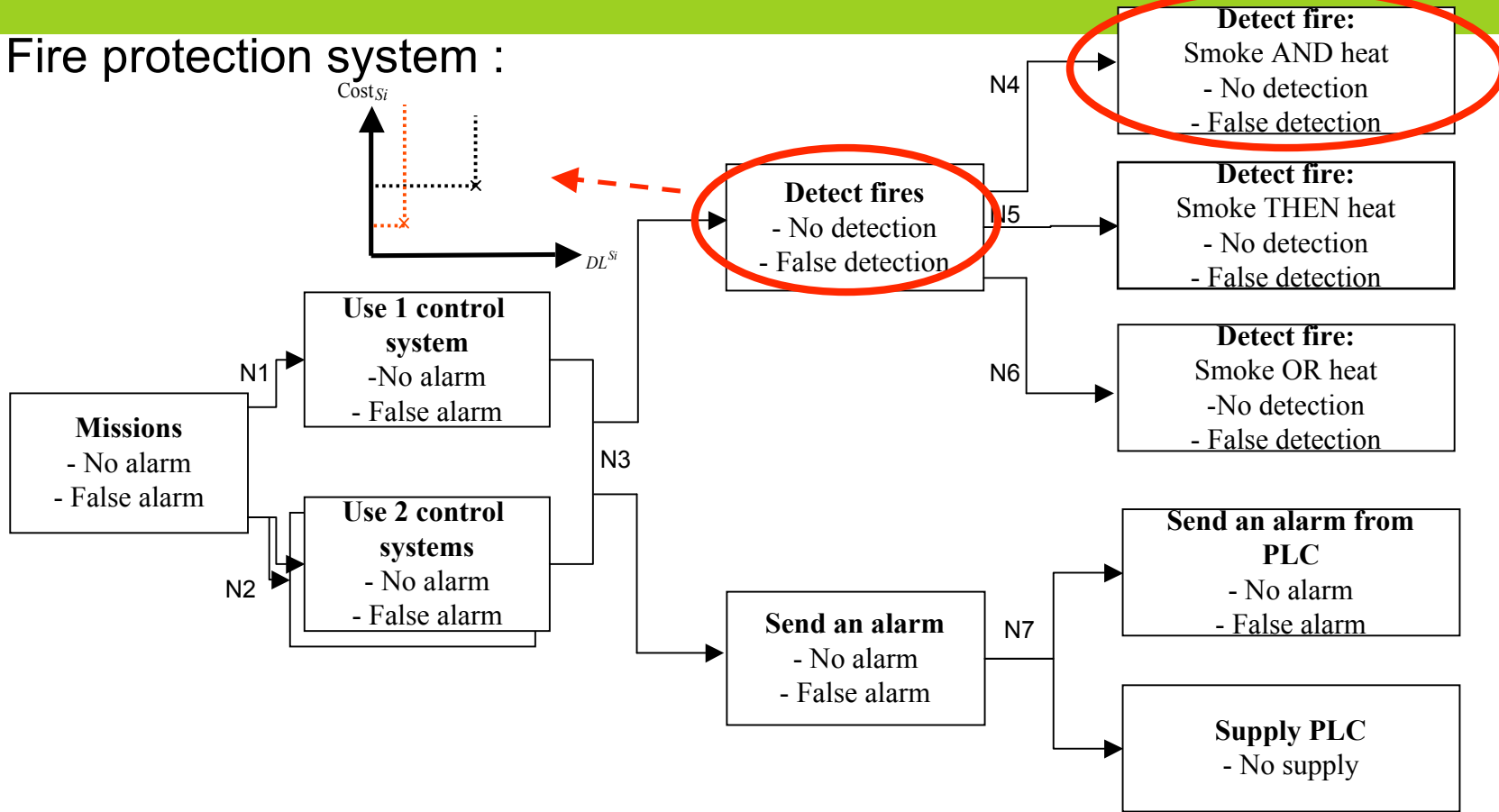
Fire protection system :



$$C_{S8} = \left\{ \text{Cost}_{S8}, (L_{\min}^{S8}, N_{\min}^{S8}) \right\}$$

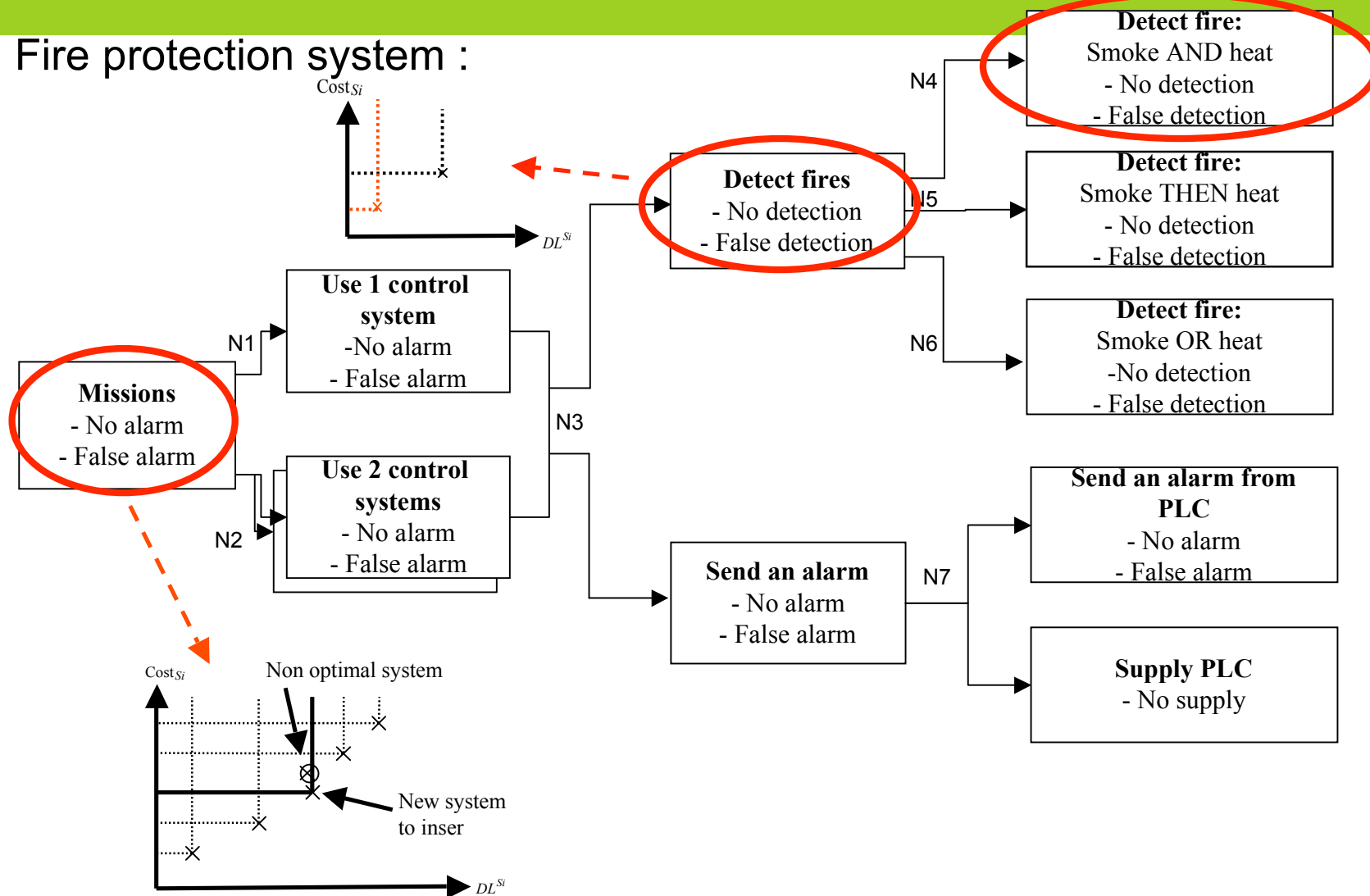
# Optimisation step

Fire protection system :



# Optimisation step

Fire protection system :



Optimal design of automated dependable system  
CLARHAUT Joffrey



# Results

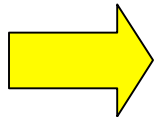
Fire protection system :

$\Omega_{\text{optimal}} = 31$  optimal control architectures

Number of optimal systems and costs		L <sub>min</sub> for dreaded event: false alarm (ER2)		
		1	2	3
L <sub>min</sub> for dreaded event: No fire alarm (ER1)	1	2 systems C : 10	4 systems C : 13 to 19	2 systems C : 20
	2	4 systems C : 13 to 19	2 systems C : 20	2 systems C : 23, 24
	3	2 systems C : 20	4 systems C : 23, 24	9 systems C : 26 to 38

# Comparison with traditional fault trees

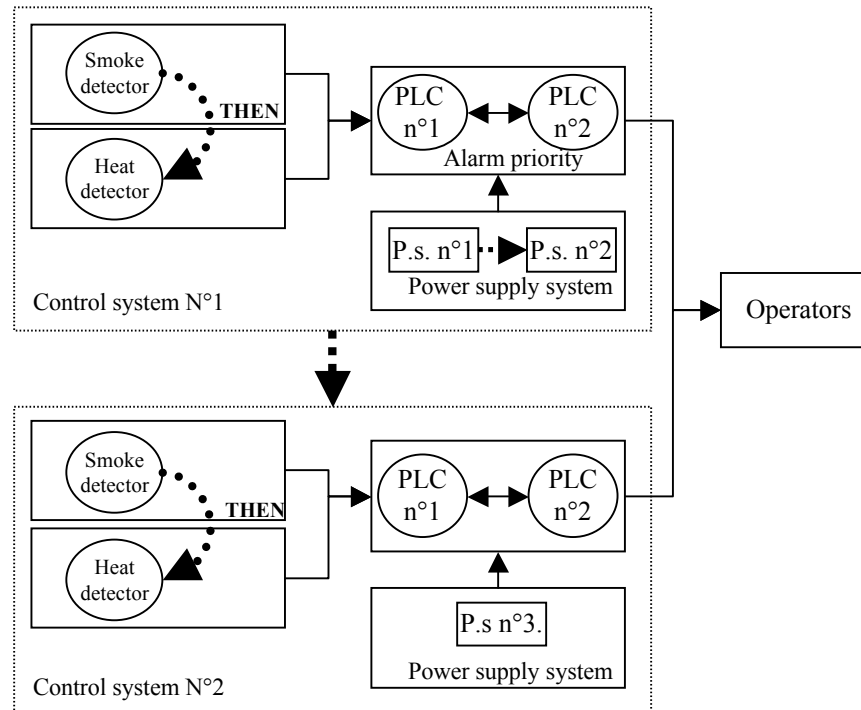
- Traditional fault trees:
  - The three types of nodes are used.
  - Only OR and AND operators are used.
- Methodology results:  
 $\Omega'_{\text{optimal}} = 54$  optimal control architectures.



Solutions obtained with the improved multi-fault tree are better: evaluation without the impossible scenarii

# Interest of scenarii

Example of optimal architecture :



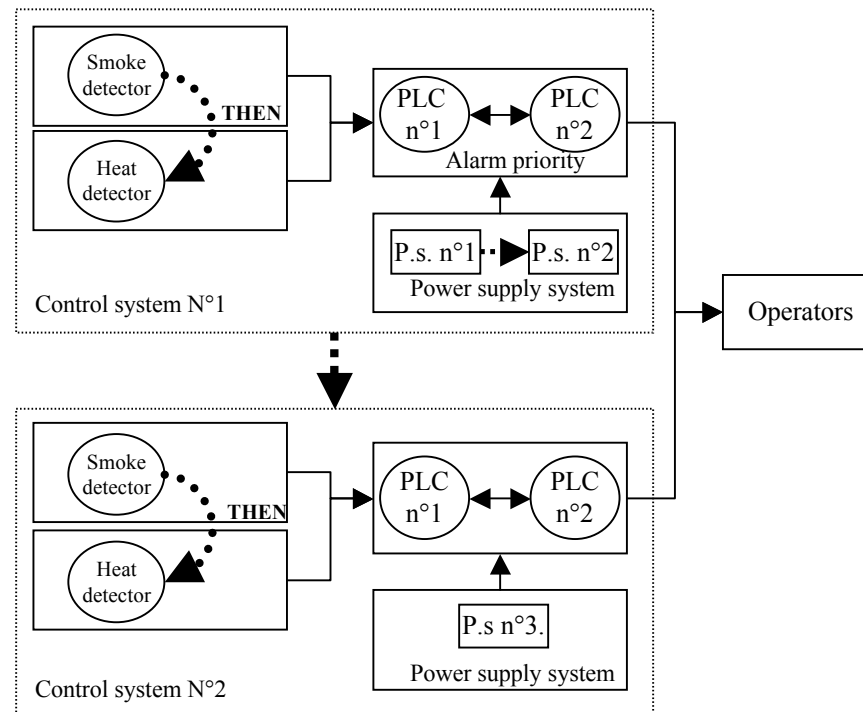
Optimal design of automated dependable system

CLARHAUT Joffrey



# Interest of scenarii

Example of optimal architecture :



Number of minimal scenarii ( $N_{min}$ ) for dreaded event « No fire alarm » (ER1):

- Traditional evaluation method : 18
- Proposed evaluation method : 12

Impossible scenario: [ Unex. Stop of power supply 2, Unex. Stop of power supply 1, Unex. Stop of power supply 3 ]

Optimal design of automated dependable system

CLARHAUT Joffrey



# Conclusion

- **Methodology interests:**
  - System's models using scenarii.
  - Set of optimized architectures characterized by a financial cost and a dependability level.
  - Can be used in the first design phases
    - obtain a first estimation of cost,
    - determine a first set of architectures.
- **Future works:**
  - Using several types of basic components (standard, smart and safe) with relative reliability coefficient.
  - Improve algorithms for huge systems.
  - Design of a software.

# Young Researchers Seminar 2009

Torino, Italy, 3 to 5 June 2009

## Optimal design of automated dependable system architectures

Application to a railroad transportation system

Thank you !!

CLARHAUT Joffrey

[joffrey.clarhaut@inrets.fr](mailto:joffrey.clarhaut@inrets.fr)

