LA SICUREZZA DEI SISTEMI COMPLESSI

SI PUÒ TENDERE AL *RISCHIO-ZERO* ?

TOMASO VAIRO

(CON L'*INVOLONTARIA* COLLABORAZIONE DI ANDREA RAPUZZI)

DataScienceSeed online #13

Data Science, Machine Learning, Artificial Intelligence Meetup a Genova

23.2.2022

Contenuto

Qualche concetto

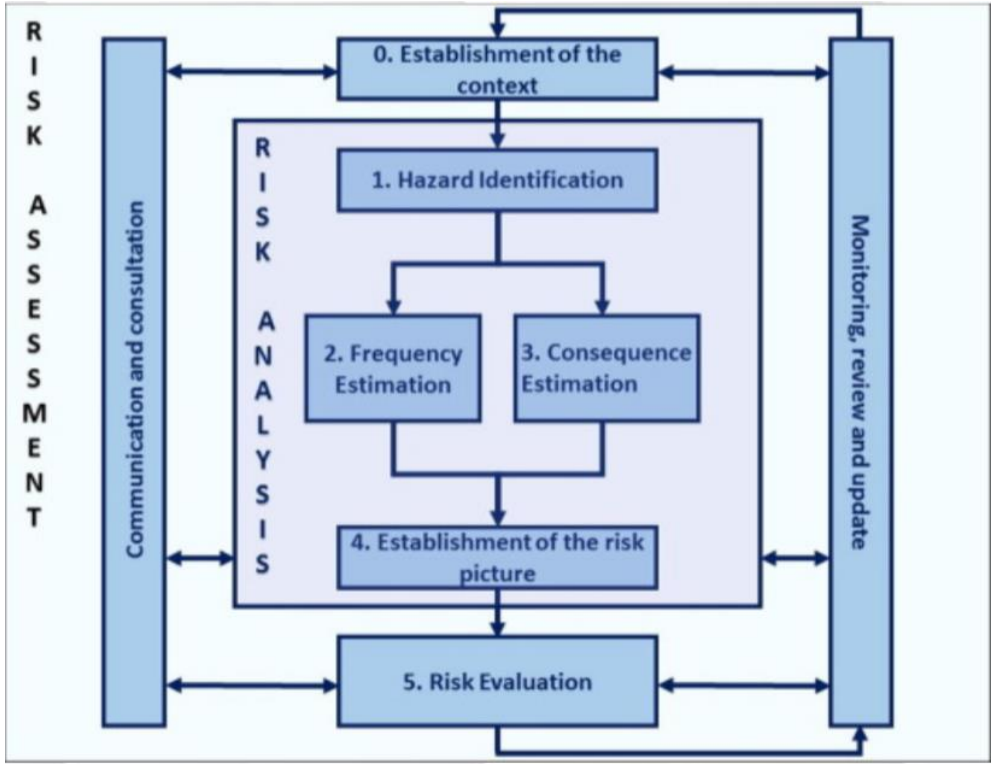
Cos'è l'analisi del rischio
Incertezza, inferenza, causalità
La necessità di un nuovo approccio

Gli strumenti

Quante evidenze servono per modificare le convinzioni?
Bayes e i ratei di guasto
Hidden Markov Model

Un esempio applicativo

L'analisi del rischio

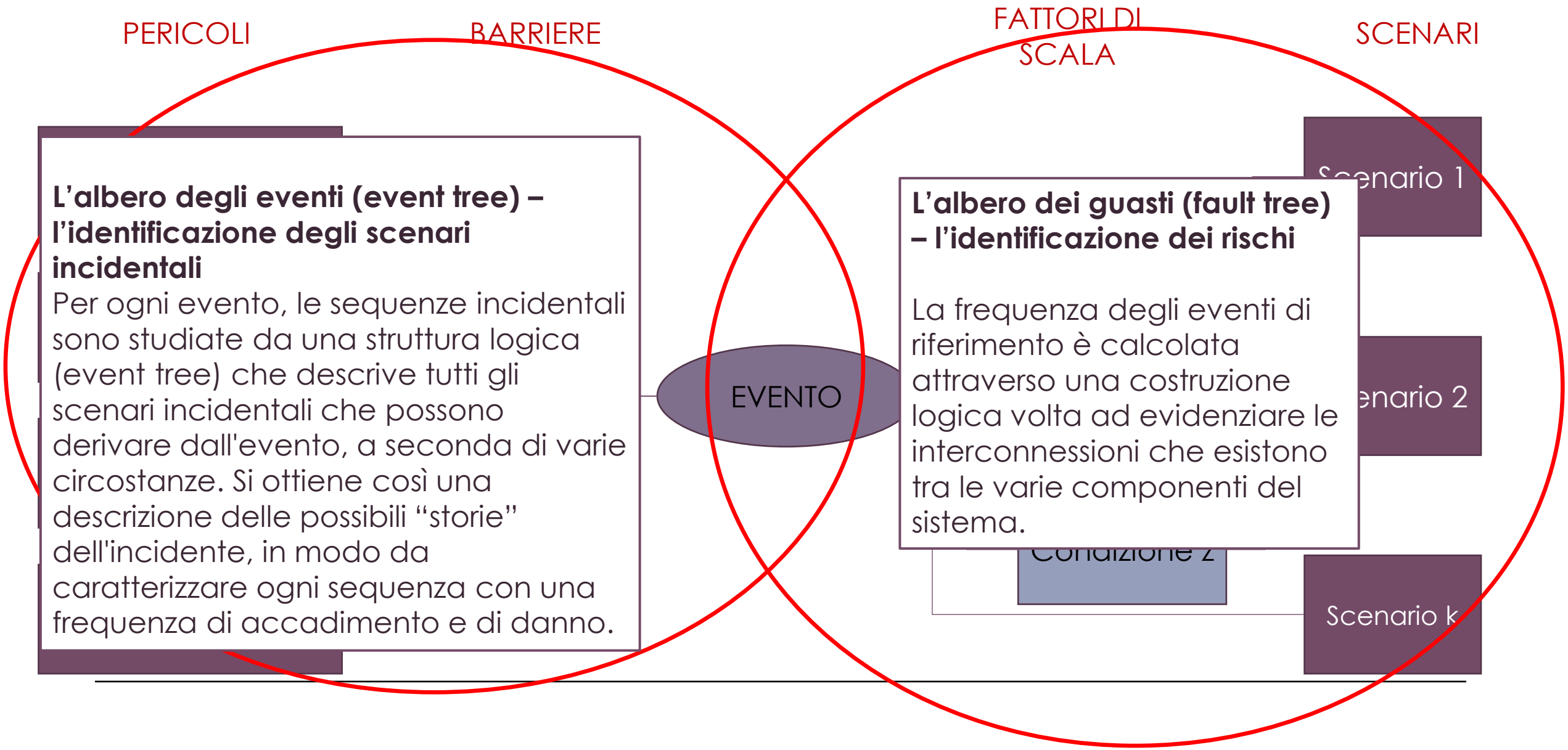


L'**analisi del rischio** è un set di metodi per investigare **i limiti di un sistema complesso** (limiti, il più delle volte, incerti)

- Perché i sistemi falliscono? (affidabilità: per scoprire le cause e i meccanismi di fallimento, e per identificare le conseguenze).
- Come sviluppare sistemi "affidabili"? (affidabili, sicuri, protetti, ...).
- Come misurare l'affidabilità? (nel design, funzionamento e gestione).
- Come mantenere l'affidabilità? (errori, individuazione, diagnosi, manutenibilità).

L'analisi del rischio è un processo di identificazione degli elementi che possono portare al rischio di un incidente (questi elementi sono chiamati **Top Events**) e di calcolo della relativa frequenza.
All'identificazione segue la valutazione delle conseguenze che i Top Events possono causare.

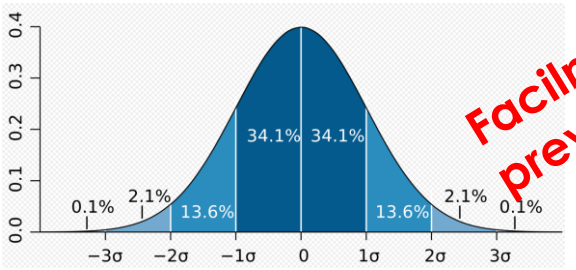
L'analisi del rischio



Incertezza, inferenza, causalità

Tre tipi di eventi inattesi…

Cigni bianchi risultano dall'incertezza 'Normale' di una distribuzione Gaussiana



Facilmente prevedibili

Cigni grigi risultano da circostanze dove l'incertezza deriva da una distribuzione di tipo Power Law (Frattale o con coda grassa)

In qualche modo prevedibili

Cigni neri risultano da tutte quelle incertezze non lineari, sulle quali non si hanno informazioni

?

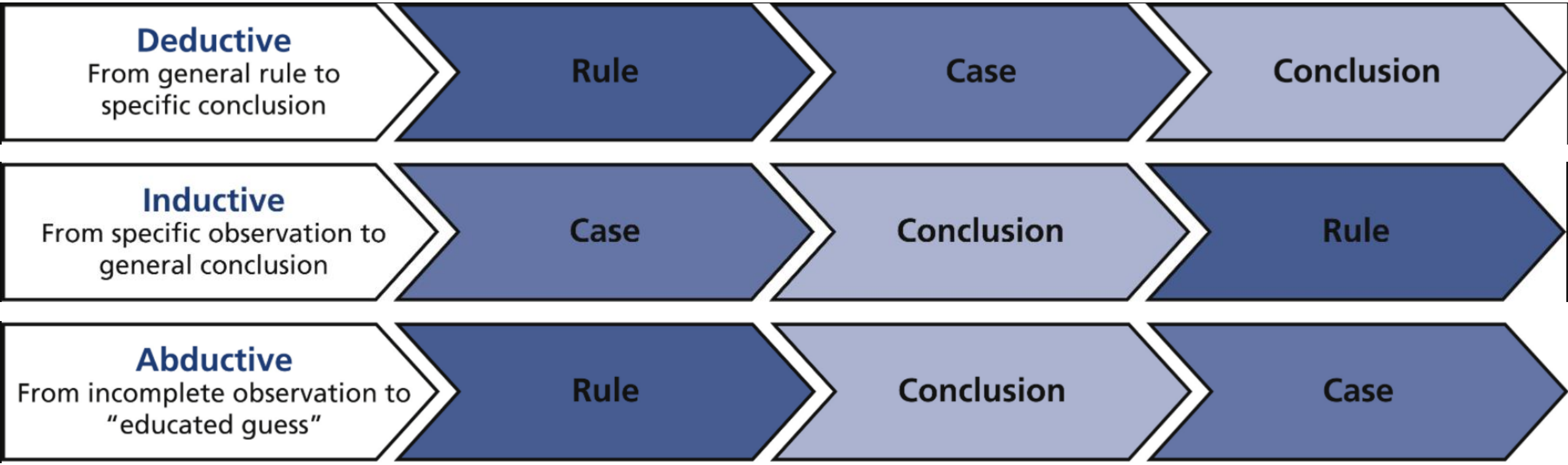
Incertezza, inferenza, causalità

DEDUZIONE

INDUZIONE

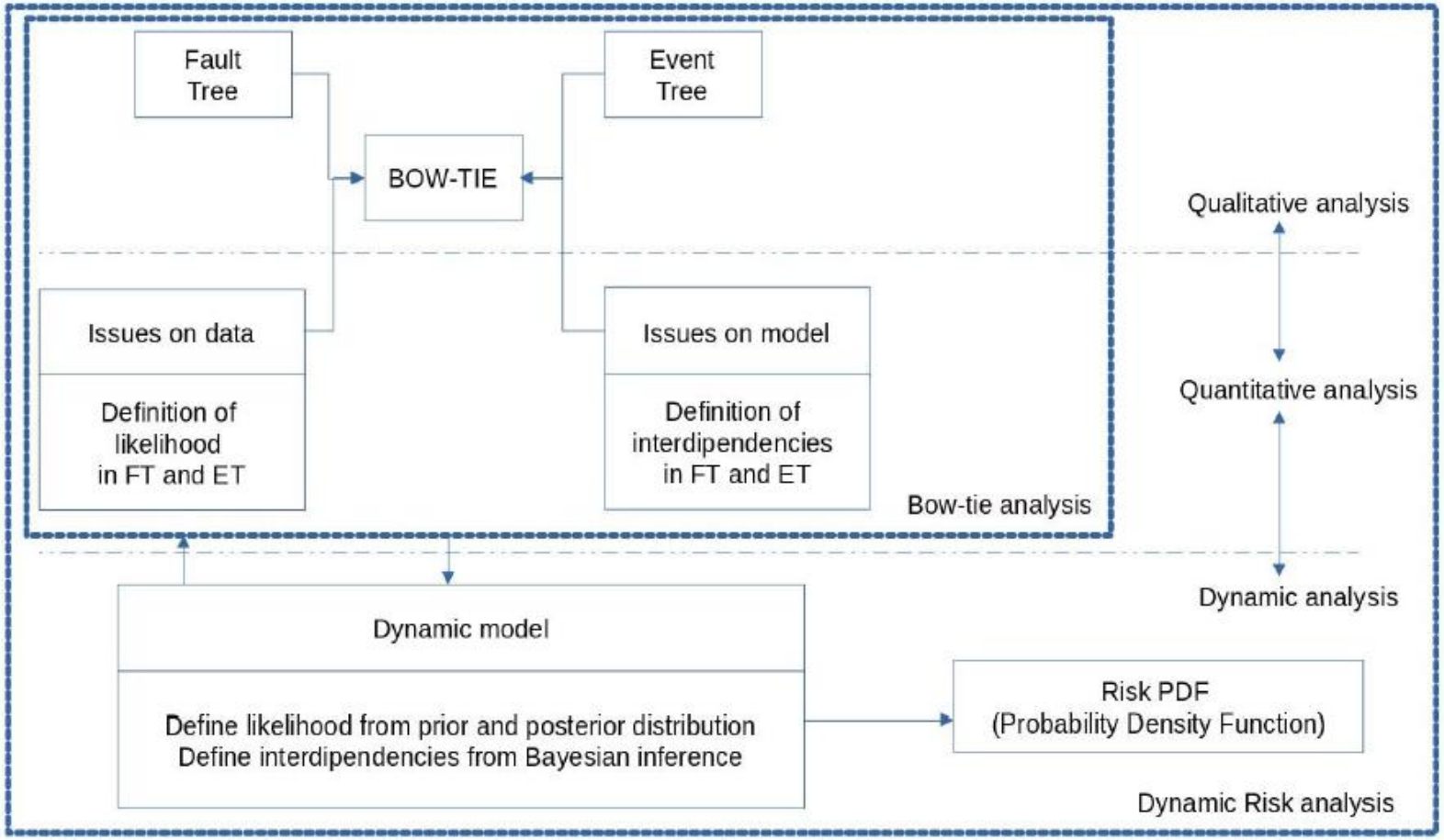
ABDUZIONE

Incertezza, inferenza, causalità



La necessità di un nuovo approccio

Perché l'analisi di rischio tradizionale fallisce?

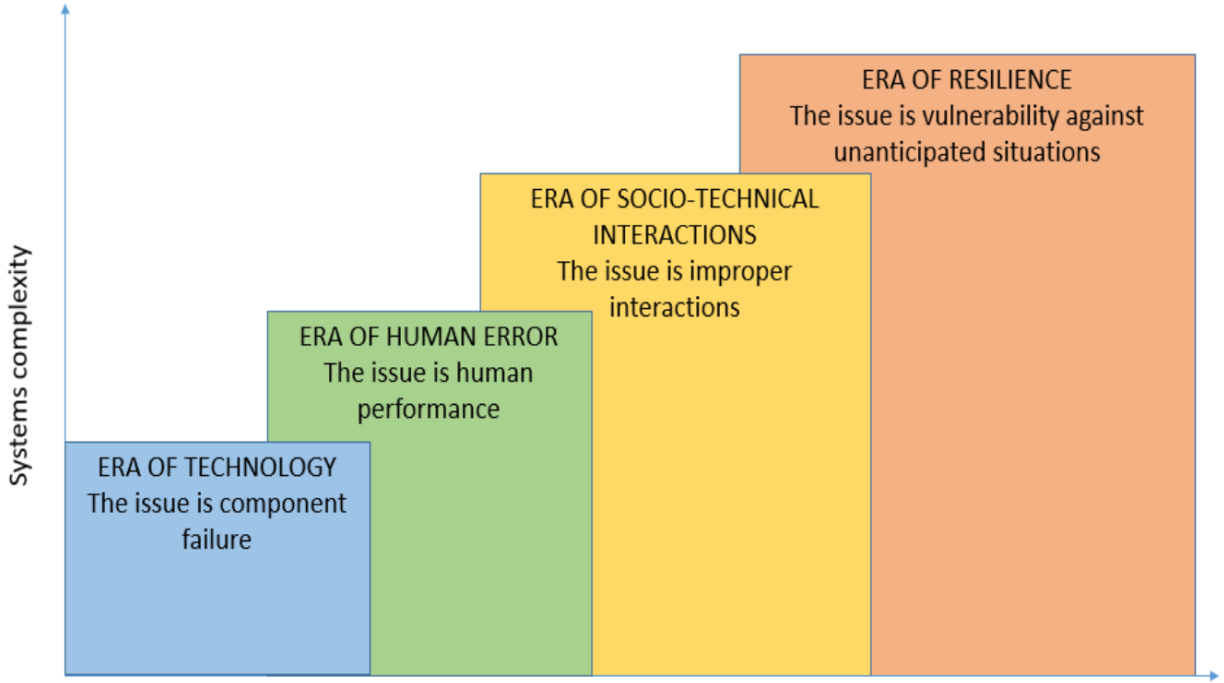


Ci sono problemi noti legati ai DATI

Incertezze legate alla rappresentatività statistica dei dati utilizati nell'analisi

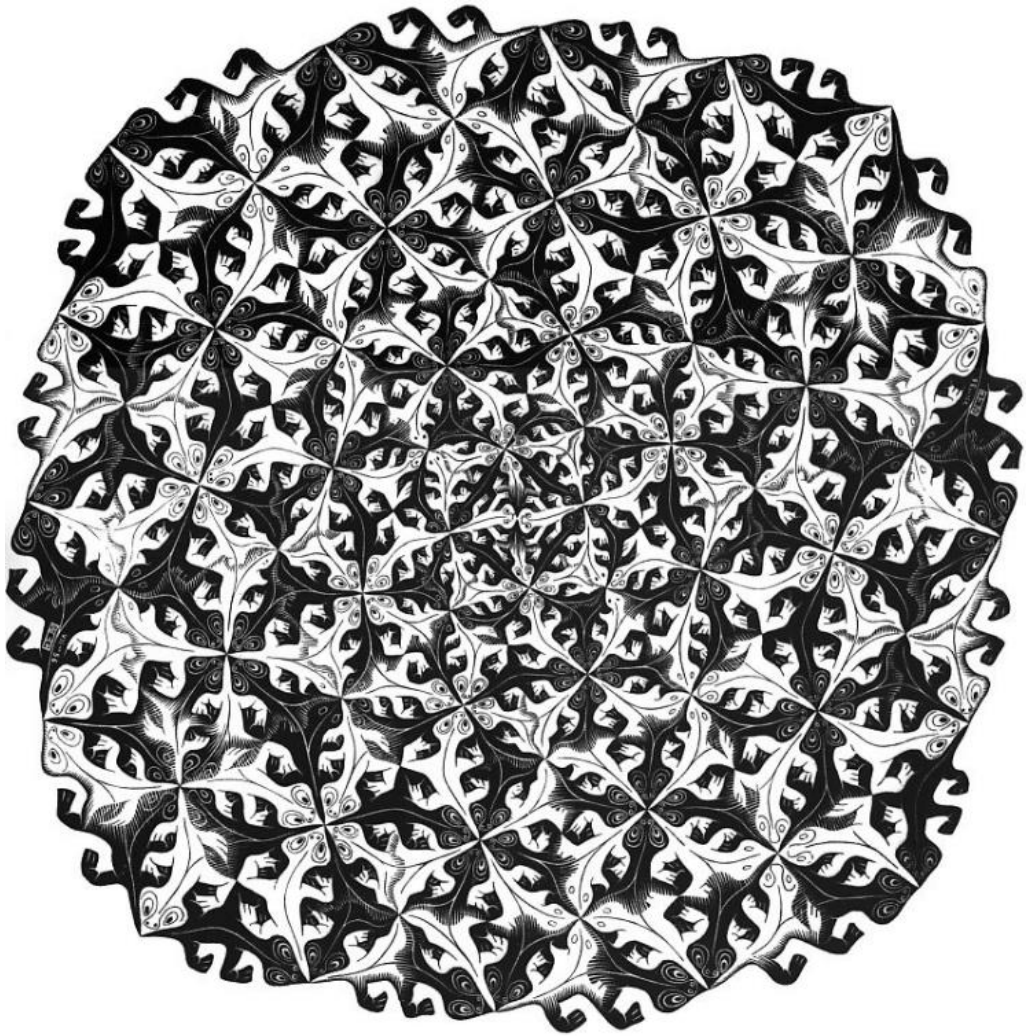
Monitoraggio in tempo reale, e predizione delle situazioni critiche

La necessità di un nuovo approccio



RA dinamica

La necessità di un nuovo approccio



Sistema: dal greco *syn* + *histánai*
mettere assieme.
Stabilire un contesto. Esplorare
la natura dell'*interdipendenza!*

Il passato è caratterizzato da
un approccio riduzionista:

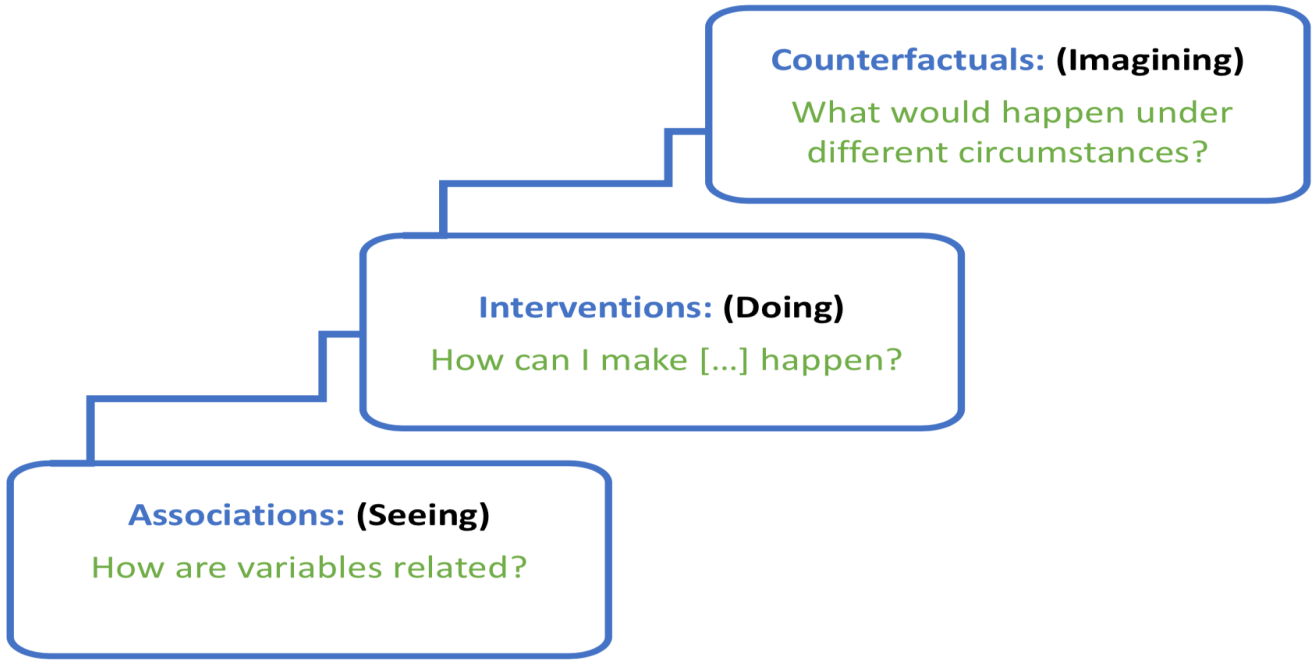
FENOMENI INDIPENDENTI –
STUDIATI SEPARATAMENTE
(es. modello domino…)

Approccio SISTEMICO

COGLIERE LE INTERCONNESSIONI E
LA RISONANZA FUNZIONALE

La necessità di un nuovo approccio

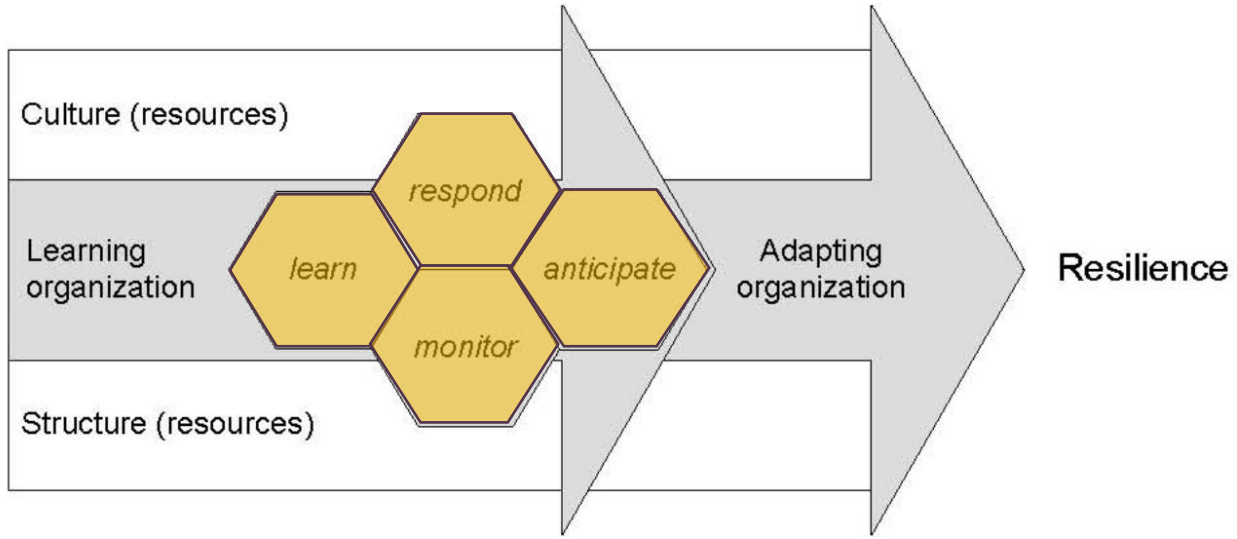
INTEGRAZIONE ???



La necessità di un nuovo approccio

L'analisi di rischio dinamica è il fondamento per l'analisi di resilienza!

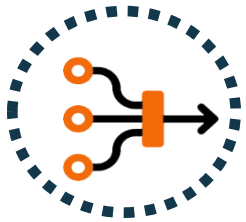
C'è bisogno di analizzare immensi quantitativi di dati, migliorare la comprensione dei processi e delle interazioni, costruire modelli predittivi affidabili e robusti.



Parole chiave:

CONTROLLARE
APPRENDERE
ANTICIPARE
RISPONDERE

La necessità di un nuovo approccio



Disponibilità di dati in tempo reale

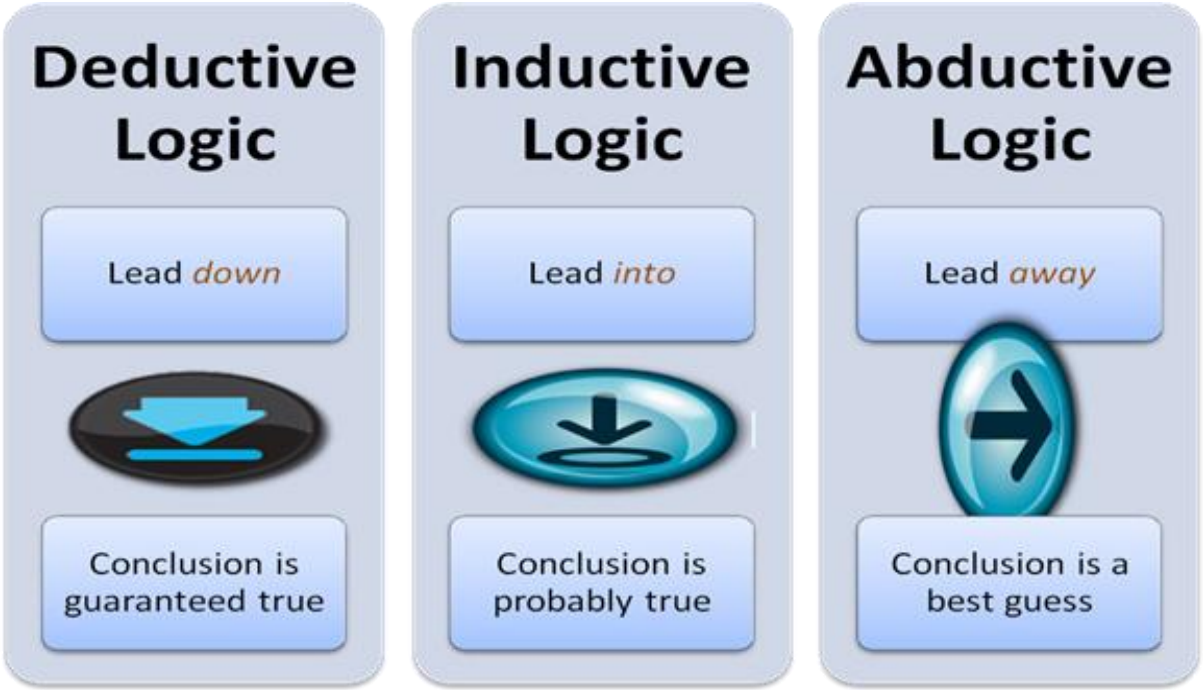
Algoritmi di ML appropriati

Modelli robusti basati su AI

La gestione della sicurezza è **immediata**! Si interviene nel **momento** in cui si identifica un evento *precursore* di una deviazione

Un evento *precursore* è un segnale "debole" del sistema, che potrebbe precedere uno o più eventi indesiderati.
La localizzazione e l'analisi dei precursori offre l'opportunità di prendere decisioni per anticipare potenziali eventi avversi.

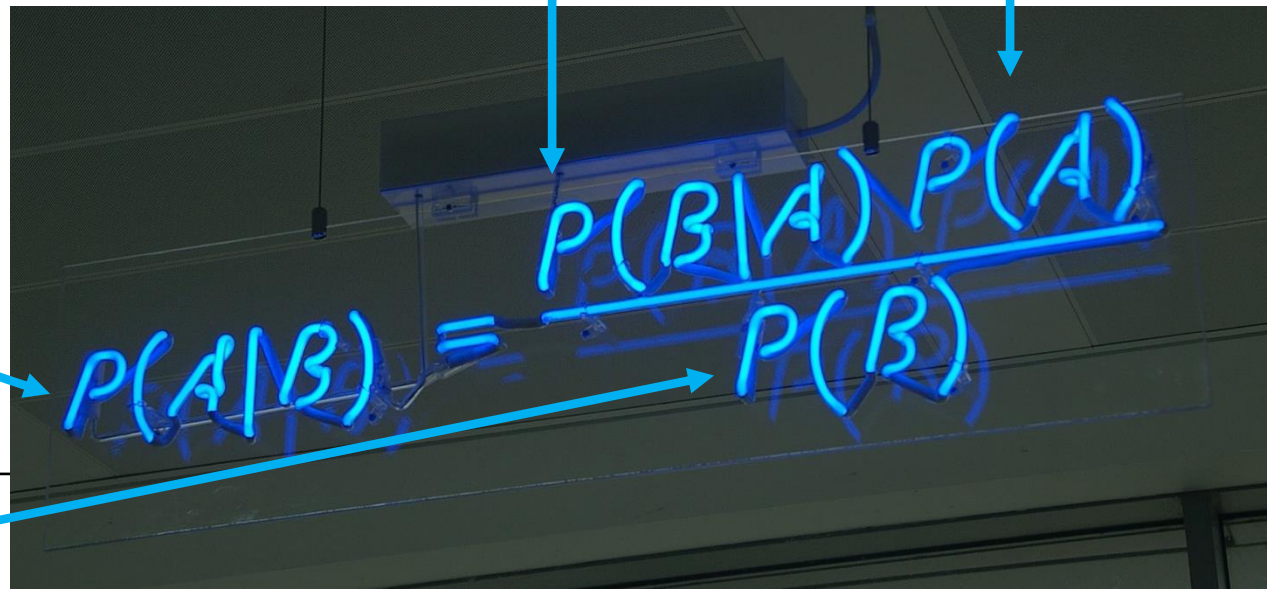
Quante evidenze servono per modificare le convinzioni?



Il teorema di Bayes

Probabilità di osservare l'evidenza (B) se l'ipotesi (A) è vera

Probabilità che l'ipotesi (A) sia vera prima di qualsiasi evidenza



Probabilità che una ipotesi (A) sia vera data l'evidenza (B)

Probabilità di osservare l'evidenza (B)

Bayes e i ratei di guasto

Le analisi ad albero dei guasti (FTA) racchiudono il concetto che il fallimento di un (sotto)sistema sia causato dal fallimento di (sotto)sistemi di livello inferiore (e quindi l'errata convinzione che interrompendo la catena si possa evitare il fallimento del sistema).

PROBLEMA:	Quantificare i fallimenti per un intero sistema è il più delle volte infattibile
SOLUZIONE PROPOSTA:	Le reti bayesiane permettono la quantificazione delle probabilità accettando le evidenze durante il funzionamento e, quindi, utilizzando il teorema di Bayes, aggiornano a posteriori, ogni volta, i ratei di guasto dei sottoelementi.

Bayes e i ratei di guasto

il rateo di guasto **λ** non è più considerato come una variabile a valore unico, ma come una **variabile casuale** espressa sotto forma di funzione di densità di probabilità (pdf). Quindi viene determinato una pdf posteriore data **E**, evidenza osservata. Questa distribuzione a posteriori può essere derivata dal prodotto di una precedente distribuzione dei valori del rateo di guasto, **f(λ)**, e la nuova informazione come funzione di verosimiglianza, **L(E|λ)** secondo:

$$f(\lambda|E) = \frac{f(\lambda)L(E|\lambda)}{\int_0^\infty f(\lambda)L(E|\lambda)d\lambda}$$

La funzione di verosimiglianza rappresenta la probabilità che **E** venga osservato dato un valore di **λ**; l'integrale al denominatore serve a normalizzare il risultato del prodotto per mantenere i valori di probabilità compresi tra 0 e 1.

Bayes e i ratei di guasto

La modellazione gerarchica Bayesiana fa uso di due concetti importanti nel calcolo delle distribuzioni a posteriori:

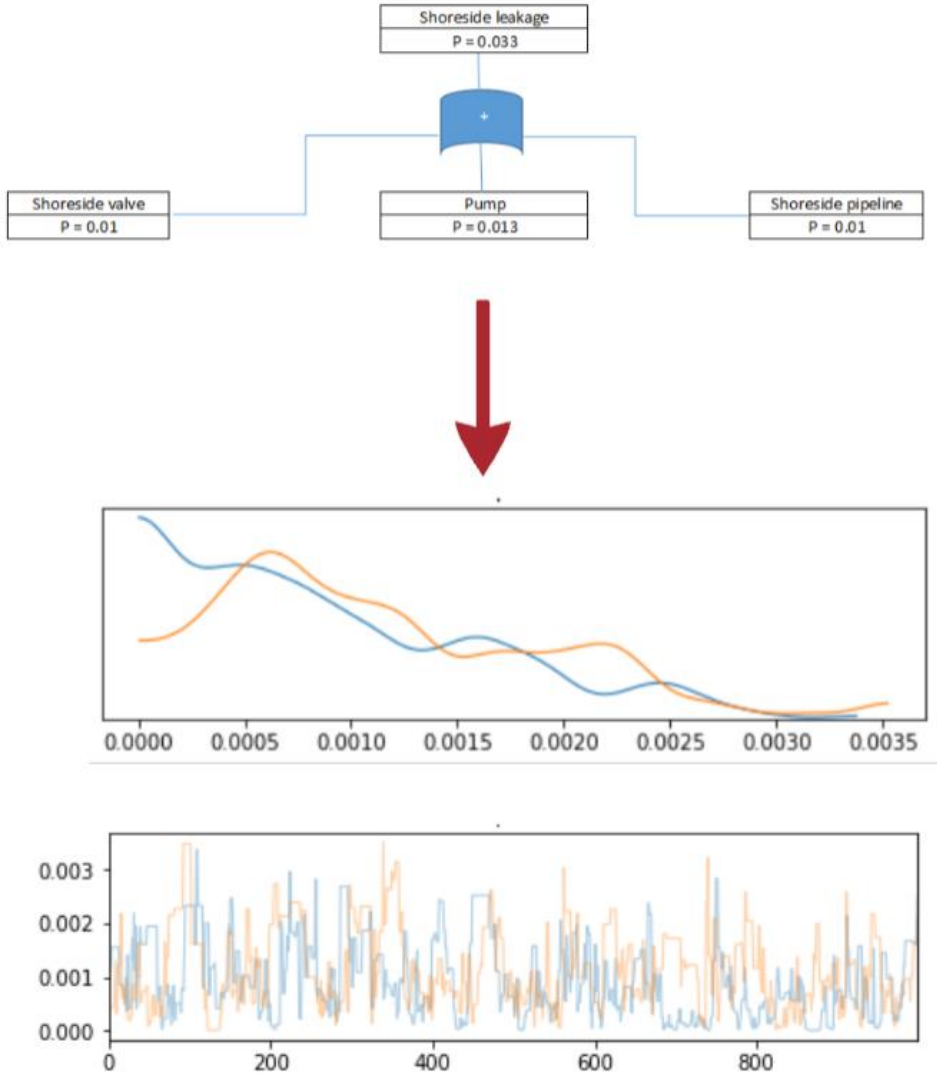
Iperparametri: parametri della distribuzione a priori
Iperprior: distribuzioni degli iperparametri

Y è una variabile casuale con distribuzione normale, con **θ** come media e 1 come varianza, ovvero **Y(θ) ~ N(θ, 1)**
Il parametro **θ** ha una distribuzione normale con media **μ** e varianza 1, ovvero **θ(μ) ~ N(μ, 1)**,
μ segue un'altra distribuzione.
μ è l'iperparametro, la sua distribuzione è un esempio di distribuzione iperprior.
La notazione della distribuzione di Y cambia quando viene aggiunto un altro parametro, cioè: **Y (θ, μ) ~ N(θ, 1)**
Se esiste un altro stadio, **μ** segue un'altra distribuzione normale con media **β** e varianza **ε**, che significa **μ ~ N(β, ε)**, anche β e ε sono iperparametri e anche le loro distribuzioni sono distribuzioni iperprior.

Il modello gerarchico bayesiano contiene le seguenti fasi:

Stadio I: yj(θj,φ) ~ P(yj | θj,φ)
Stadio II: θj(φ) ~ P(θj, φ)
Stadio III: φ ~ P(φ)

La verosimiglianza, come si vede nello stadio I, è **P(yj | θj,φ)**, con **P(θj,φ)** come sua distribuzione a priori.
La verosimiglianza dipende da **φ** solo attraverso **θj**.



Bayes e i ratei di guasto

La distribuzione a priori della fase I può essere suddivisa in:

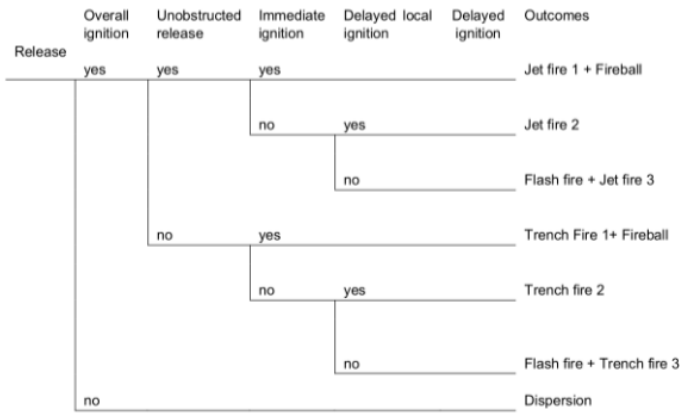
P(θj,φ) = P(θj | φ) P(φ) [dalla definizione di probabilità condizionata]

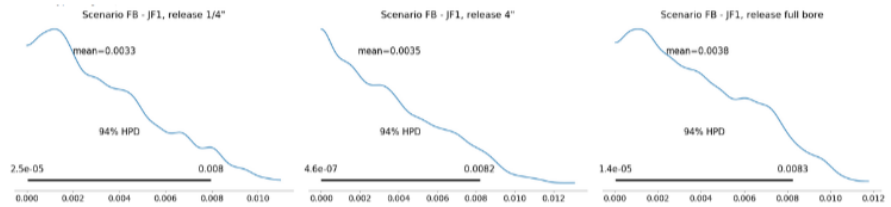
Con **φ** come suo iperparametro con distribuzione iperprior **P (φ)**.

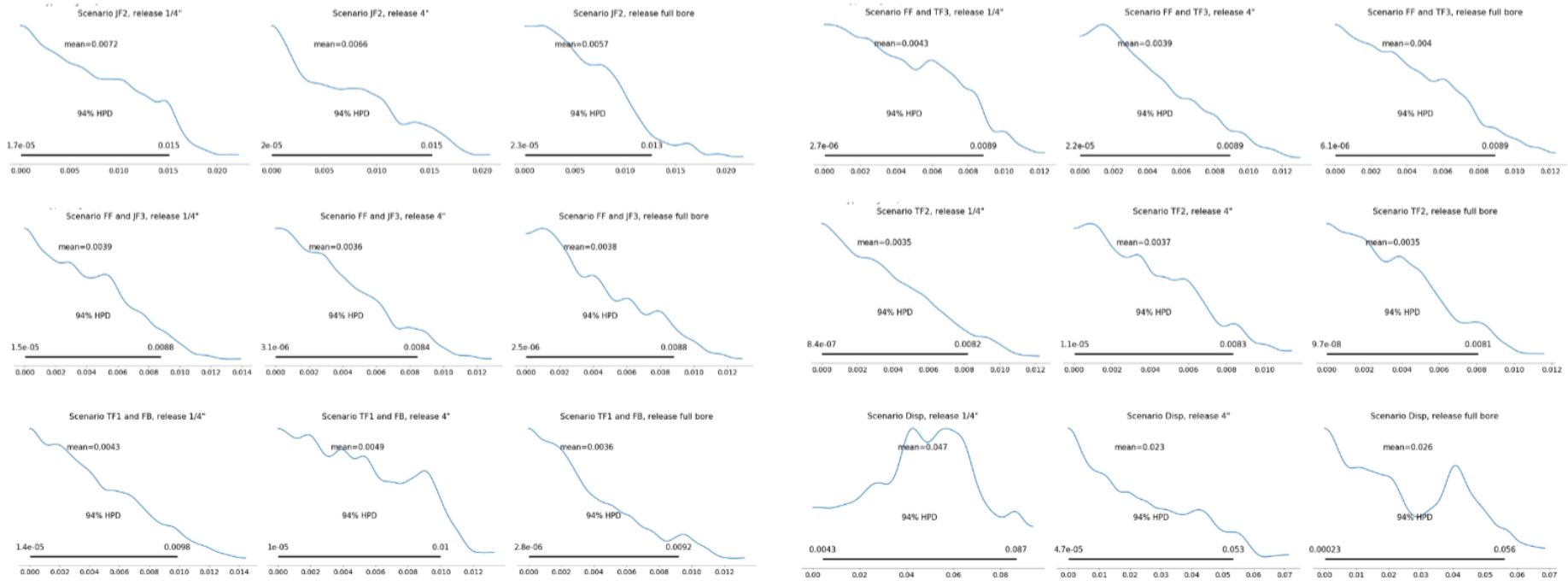
Pertanto, la distribuzione a posteriori è proporzionale a:

P(φ,θj | yj) ~ P(yj | θj,φ) P (θj,φ) [usando il teorema di Bayes]
P(φ,θj | yj)i ~ P(yj | θj) P(θj | φ) P(φ)

Hole size	FB JF1	JF2	FF JF3	TF1 FB	TF2	FF TF3	Disp.
1/4"	8.9E-9	1.3E-5	1.3E-6	2.7E-7	3.9E-5	3.9E-7	4.3E-2
4"	1.1E-7	2.7E-4	2.3E-7	6.2E-8	1.4E-4	1.4E-7	4.6E-2
full	7.0E-4	9.9E-3	1.0E-3	4.1E-4	5.8E-3	6.2E-4	0

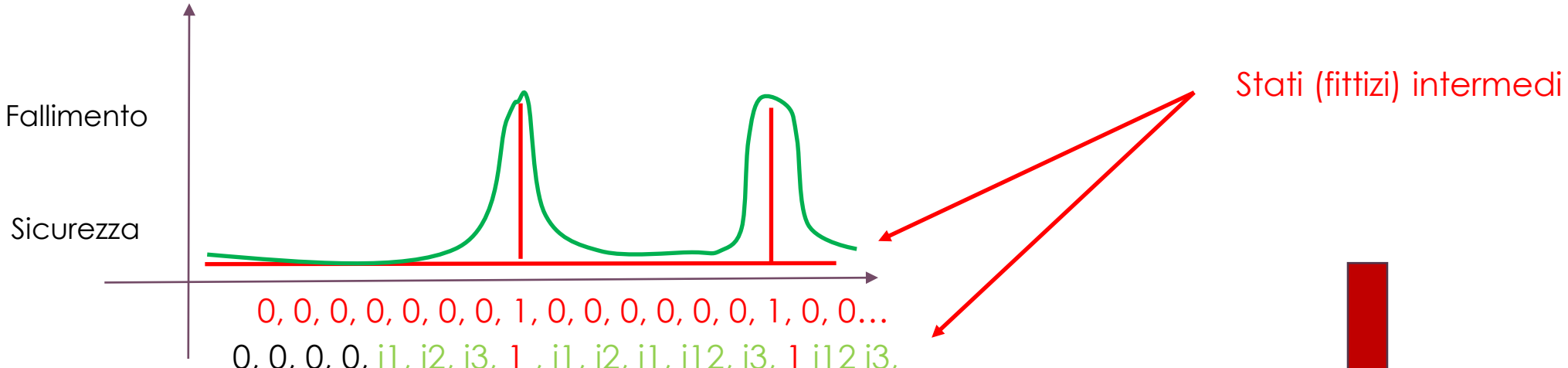


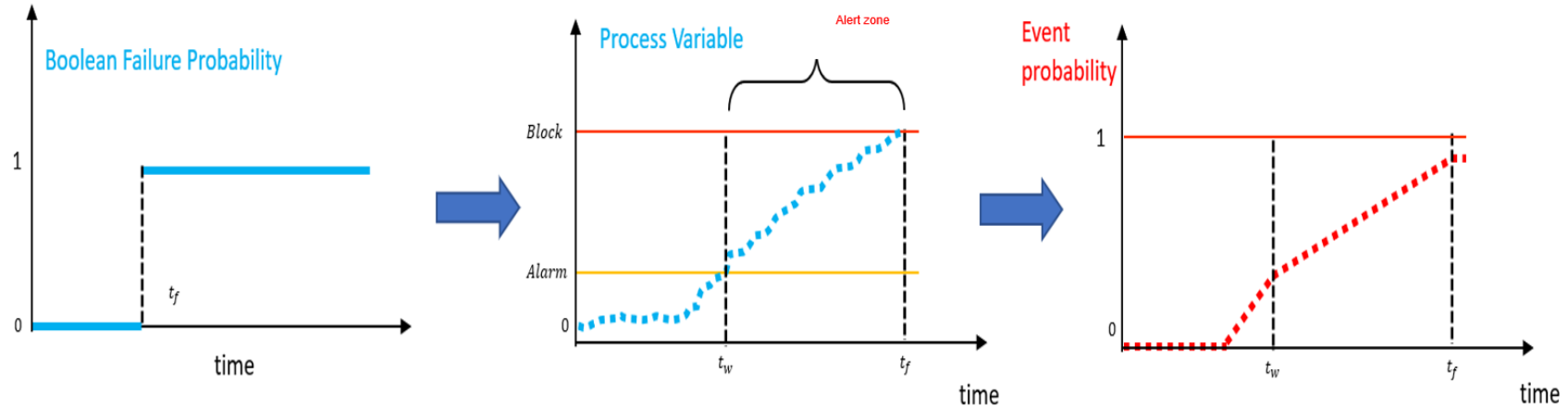




Hidden Markov Model

Però… provando a predire i fallimenti di un sistema…





FTA boolean failures

Process variables set-points

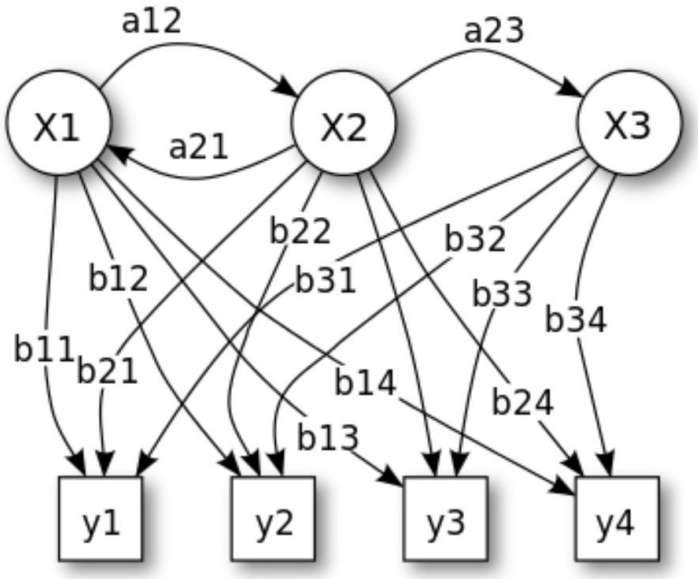
Dynamic process control

Hidden Markov Model

Si assume che il sistema possa essere rappresentato da un **processo di Markov –X** – con **stati non osservabili ("hidden")**.
Si assume anche che ci sia **un altro processo Y** il cui comportamento "dipende" da X.

L'obiettivo è conoscere X osservando Y.

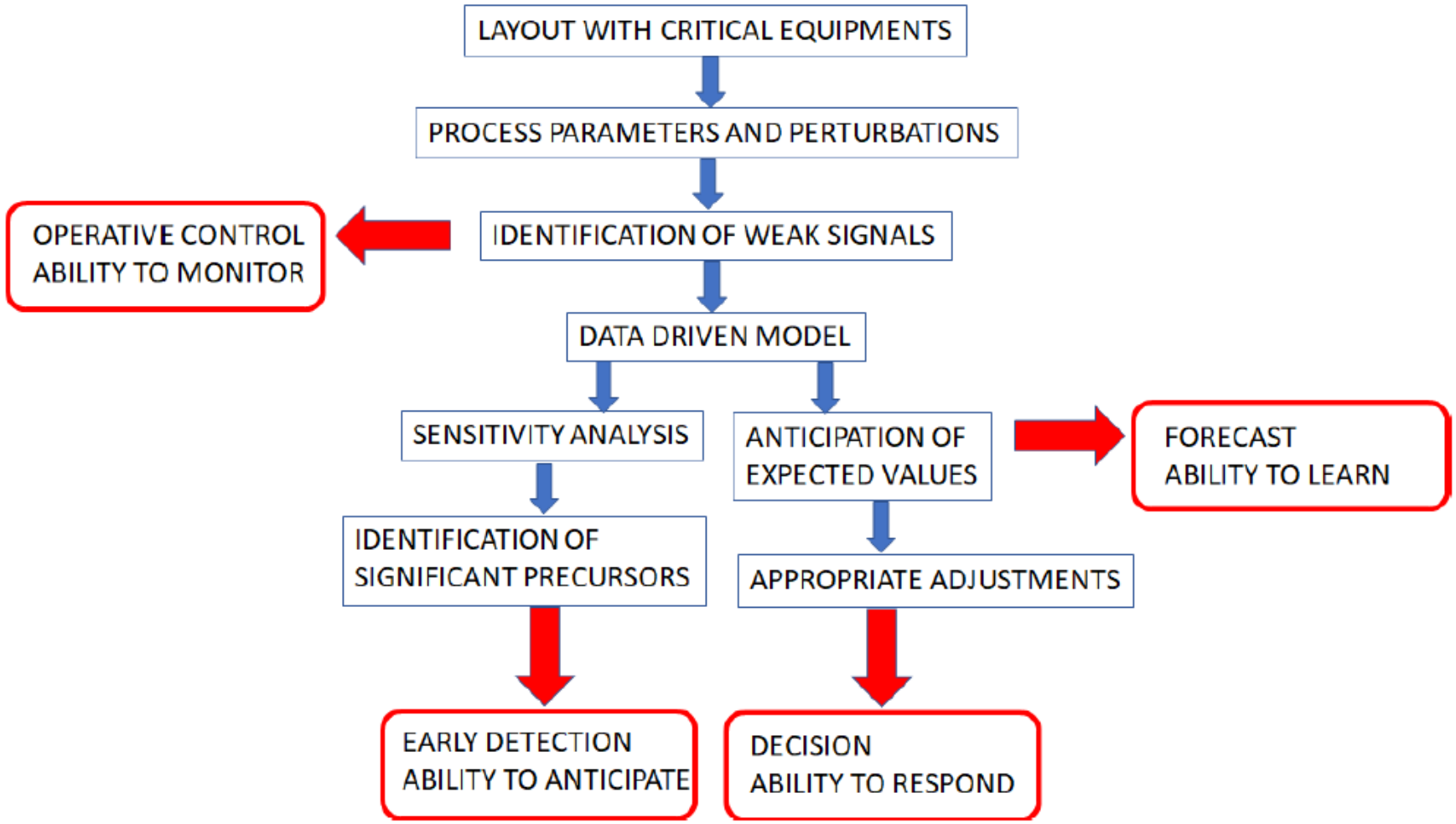
l'esito di Y all'istante t_0 può essere "influenzato" esclusivamente dall'esito di X a t= t_0 e gli esiti di X e Y a t< t_0 non devono influenzare l'esito di Y a t= t_0



Parametri probabilistici di un Hidden Markov Model

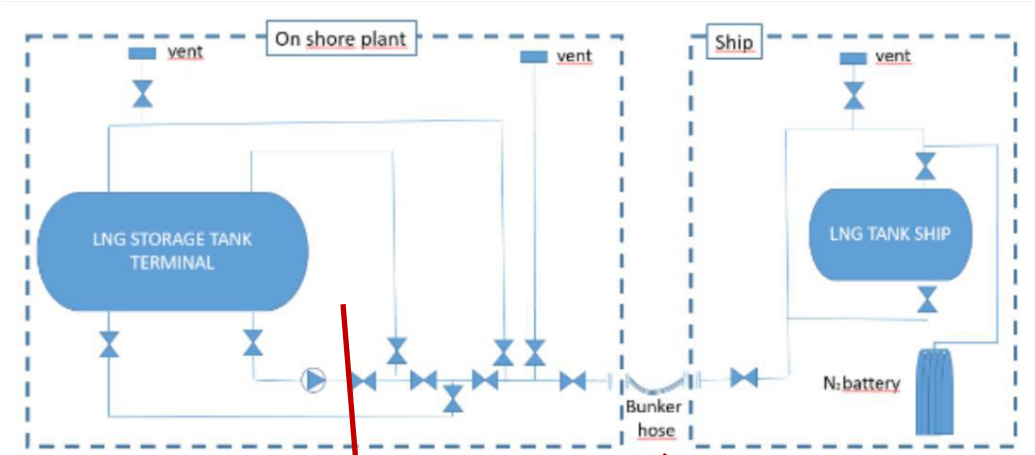
X — stati (non osservabili)
y — osservazioni possibili
a — probabilità di transizioni tra stati
b — probabilità degli stati date le osservazioni

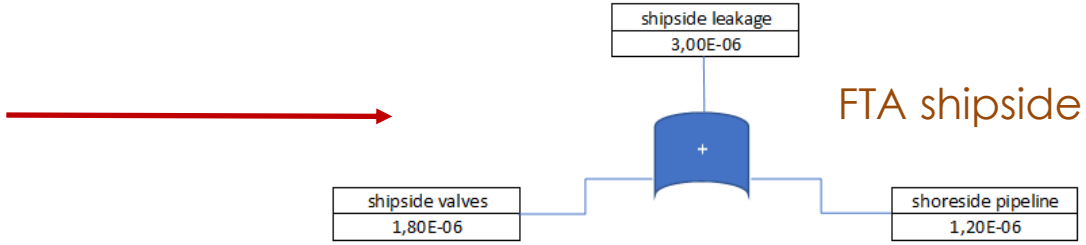
Un esempio applicativo



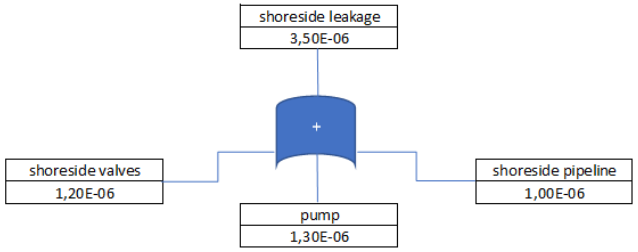
Un esempio applicativo

Bunkeraggio di GNL

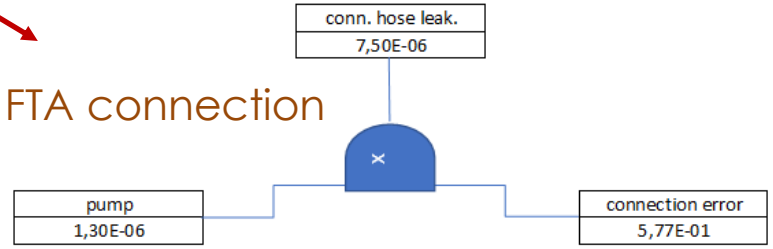




FTA shipside



FTA shoreside



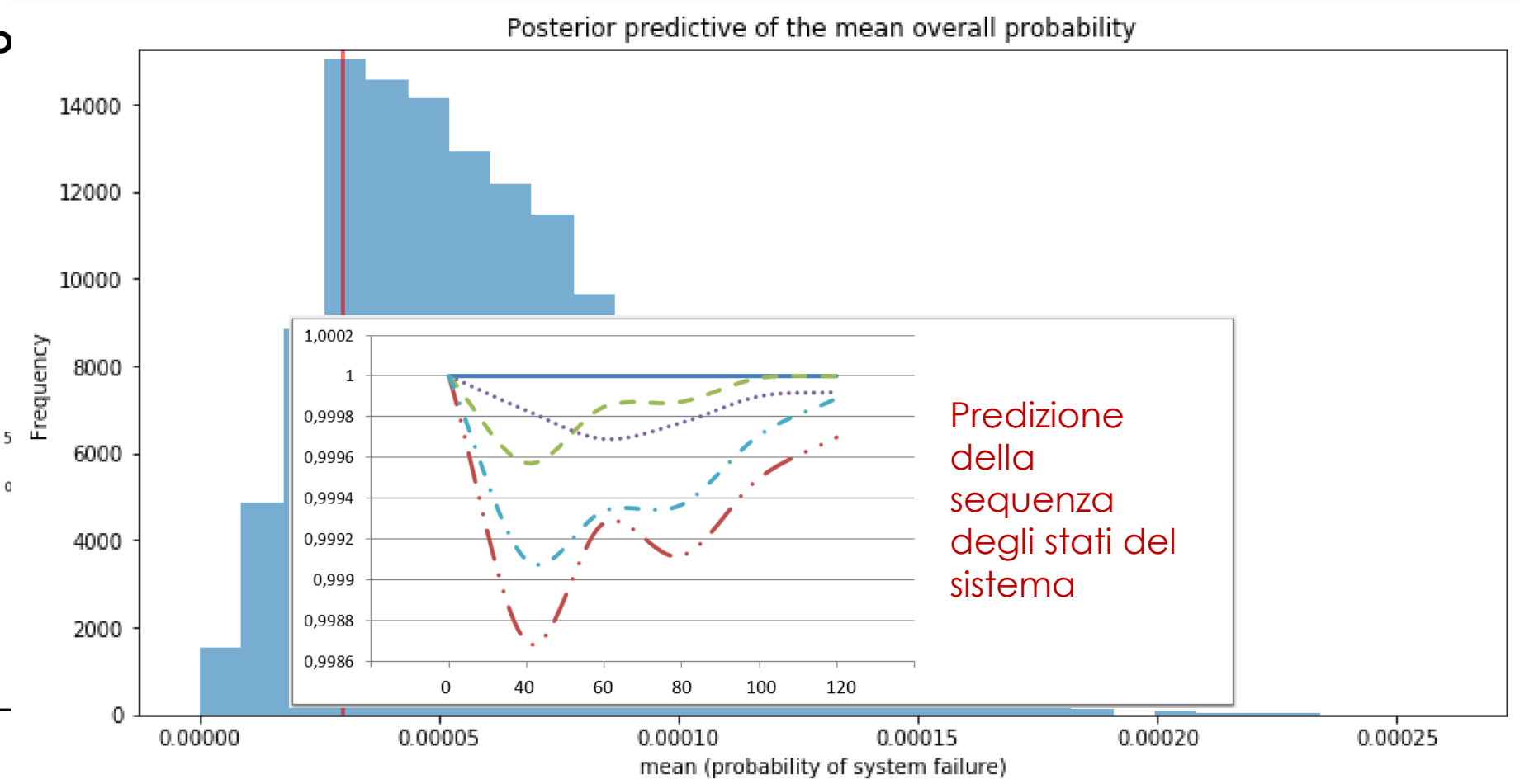
FTA connection

Un esempio applicativo

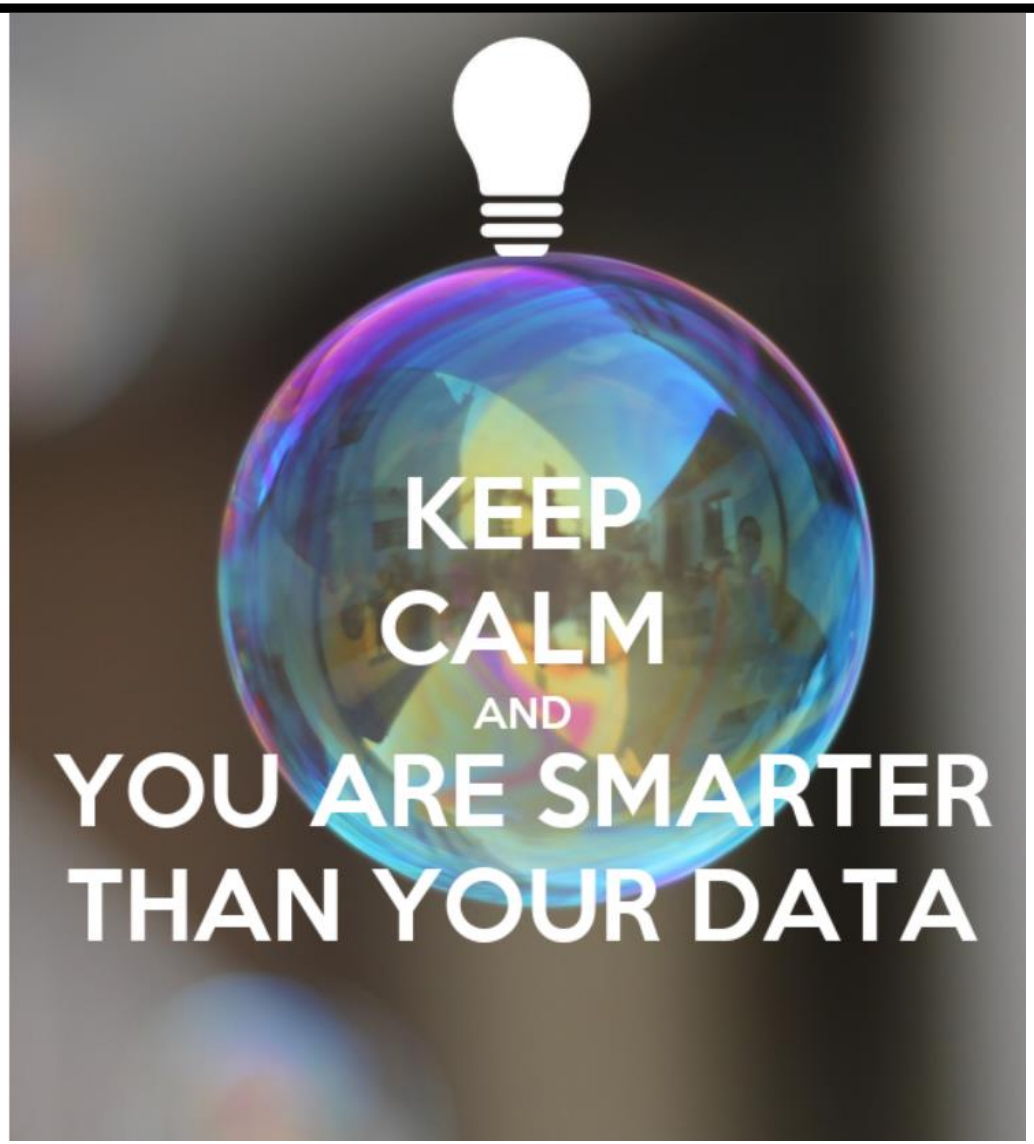
Bunkeraggio di GNL

Le distribuzioni a posteriori dei precursori, aggiornate ad ogni nuova evidenza...

Raccontano **derato**



GRAZIE!!!



Tomaso Vairo