Resilience assessment of safety-critical systems

Hector Diego Estrada-Lugo[1]

Dr. T.V. Santhosh[1], Dr. Marco De Angelis[1], Prof. Edoardo Patelli[2]
[1] University of Liverpool
[2] University of Strathclyde

H.D.Estrada-Lugo@liverpool.ac.uk

4/11/2020

Performance of complex engineered systems

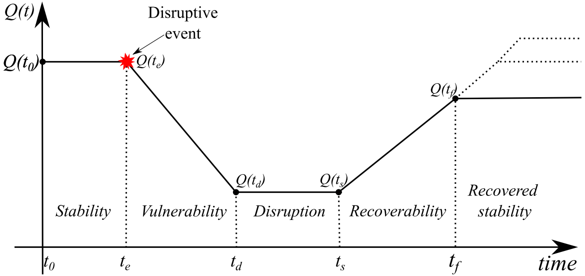
- Understanding and management of complex engineering systems is key.
- Ensure operational performance even with disruptive events or harsh operating conditions.
- Need of effective and novel approaches for risk assessment and recovery management.

Resilience quantification

Resilience is the ability of a system to survive and recover from the likelihood of damage due to disruptive events [1].

$$R(t_r|e_i) = \frac{Q(t_r|e_i) - Q(t_d|e_i)}{Q(t_0) - Q(t_d|e_i)}$$

Where, $Q(t_0)$: initial performance (before disruptive event, e_i);
$Q(t_r|e_i)$: Restored system;
$Q(t_d|e_i)$: Disrupted system.



[1] Estrada-Lugo, H.D., T.V. Santhosh, M. De Angelis, & E. Patelli. Resilience assessment of the safety-critical systems with credal networks. In Proceedings of the 30th ESREL conference and the 15th PSAM Conference. November 2020.

Resilience assessment

Need of decision making tools that take into account:

- Randomness of potential threats.
- Model accuracy and increasing complexity in highly interconnected systems.
- Human and organisational factors.
- Variability on time of system performance.
- Epistemic uncertainty.

A few techniques in literature:

- Fault Tree and Event Tree Analyses (dependability).
- Dynamic Bayesian Networks, Survival signature, Petri-nets (time dependence).

However, there is something missing...

Epistemic Uncertainty

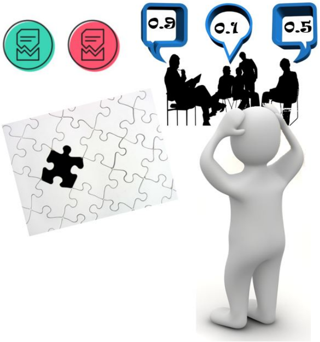
Uncertainty related to indeterminacy, ambiguity, fragmentary or dubious information and other phenomena, which do not support the analyst in forming a subjective opinion in terms of probabilities [2].

Sources:

- Lack of knowledge or poor data.
- Linguistic expressions.
- Contradictory information.
- Differences between expert judgements.

Adopt imprecision to avoid:

- Hard assumptions.
- Excessive simplification of models.
- Over or underestimated outcomes.

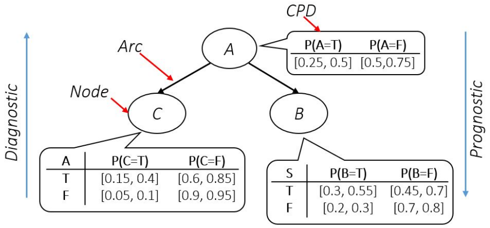


[2] Beer, M., Ferson, S., & Kreinovich, V. (2013). Imprecise probabilities in engineering analyses. Mechanical systems and signal processing, 37(1-2), 4-29.

What is a Credal Network?

Probabilistic graphical model to study and analyse the genuine dependencies of uncertain and imprecise parameters.

- **Nodes**: Events.
- **Arcs**: Causality or dependency.
- Nodes can be **Boolean** or **multi-state**.
- A **Child** node depends on at least one **Parent** node.
- **Root** nodes: No parents.
- **Prediction** and **diagnostic** analyses.
- Accept wide range of information.



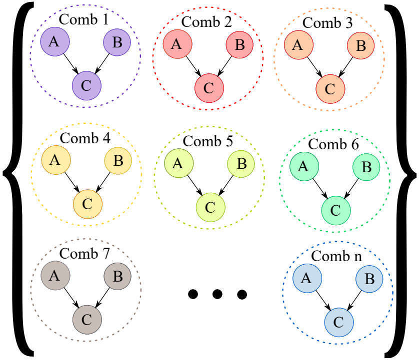
- Aleatory uncertainty: Random variables (probabilities).
- Epistemic: Credal sets (intervals).

Credal sets

- A credal set $K(X_i \mid \pi_i(X_i))$ is a closed set of probability densities $P(X_i \mid \pi_i(X_i))$.
- Each vertex of the set $K(X_i)$ is known as extreme point.
- All the possible combinations of extreme points are given by the closed convex hull of $K(X_i)$, the joint credal set:

$$K(X_i) = CH\left\{P(X_i) : P(X_i) = \prod_{i=1}^{n} P(x_i|\pi_i)\right\}$$

- Thus, a CN contains a finite set of Bayesian networks.

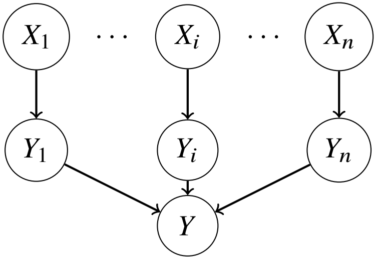


π_i parent nodes of variable X_i,
n: variables in network

Building priors: Imprecise Noisy-MAX

Imprecise Noisy-MAX is a canonical model to train a CN from a limited number causal assumptions (e.g., component failure probability) [3].

$$\underline{P}(Y = y|X_i) = \begin{cases} \underline{P}(Y \leq 0|X_i) & if \;\; y = 0, \\ \underline{P}(Y \leq y|X_i) - \overline{P}(Y \leq y-1|X_i) & if \;\; y > 0. \end{cases}$$



X_i: cause variable,
Y_i: inhibitor of variable Y.

Where,

$$\underline{P}(Y \leq y|X_i) = \prod_{i=1}^{n} \sum_{y=0}^{y} \underline{q}_{i,y}^{x_i}$$

Here, $\underline{q}_{i,y}^{x_i} = \min P(Y = y|X_i = x_i, X_j = 0, \;\; \forall\, j, j \neq i)$. Similarly for the upper bound.

---

[3]Estrada-Lugo, H.D., De Angelis, M., & Patelli, E. Fault Trees into Credal networks adopting imprecise Noisy-MAX. In Proceedings of the International Symposium on Imprecise Probabilities: Theories and Applications. July, 2019.

Dynamic credal networks

Dynamic behaviour can be represented by introducing relevant temporal dependencies.

$$K(X_i) = CH\{P(X_i^t)\}$$

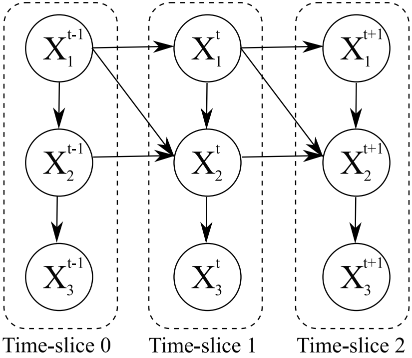
Adopting the Markov condition for a variable X in different time-slices:

$$X^{t+1} \perp X^{0:t-1} | X^t$$

Then,

$$P(X_i^t) = \prod_{i=1}^{n} \prod_{t=0}^{\tau-1} P(X_i^{t+1} | \pi_i^t)$$

Where, τ: last time-slice.



Probabilistic inference

Computing the posterior probability ($P(x_q)$) from prior information, $P(x_i|\pi_i)$ and evidence, $P(x_e)$ with Baye's Theorem. Key for **diagnosis** and **prognosis**.

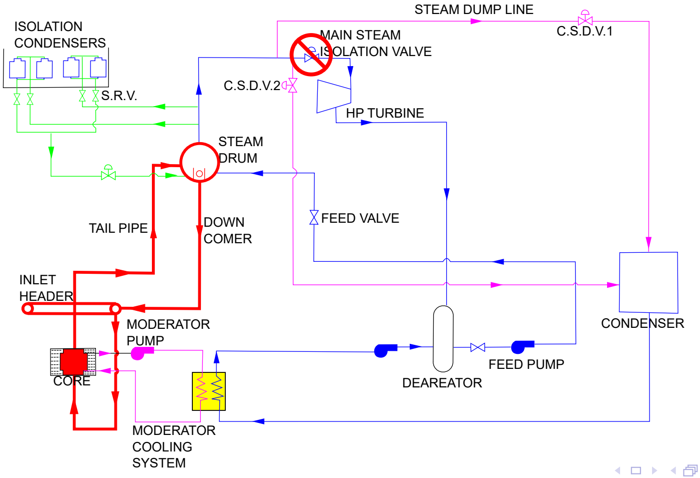
$$\underline{P}(x_q|x_e) = \min_{P(X_i|\pi_i)} \frac{\sum_{U \backslash x_q, x_e} \prod_{i=0}^{n} P(x_i|\pi_i)}{\sum_{U \backslash x_e} \prod_{i=0}^{n} P(x_i|\pi_i)}$$

$$\overline{P}(x_q|x_e) = \max_{P(X_i|\pi_i)} \frac{\sum_{U \backslash x_q, x_e} \prod_{i=0}^{n} P(x_i|\pi_i)}{\sum_{U \backslash x_e} \prod_{i=0}^{n} P(x_i|\pi_i)}$$

With $P(X_i|\pi_i) \in K(X_i|\pi_i)$ inside the variable universe $U = x_1, \ldots, x_n$.
Complexity and computational time escalates exponentially with the number of variables.

Case study: Advanced Thermal Reactor

Disruption in Main Steam Isolation Valve causes pressure increase in Main Heat Transport System if not controlled.

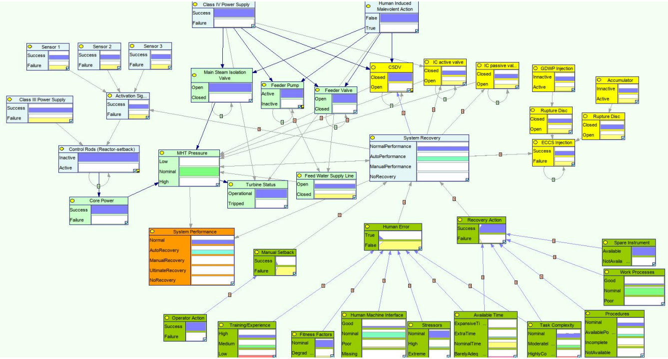


Modelling Main Heat Transport System

Prior probabilities are obtained from technical reports [4].

Human Error Probabilities from SPAR-H method [5].

Component (code)	Failure probability	Repair time (min)
Control Rods (OCCAE)	[*1.1e-7* , *4.0e-7*]	120
CSDV (VWDAF)	[*1.7e-5* , *3.1e-5*]	12
MSIV (VRAAE)	[*1.2e-6* , *2.4e-6*]	0.6
SRV (VCAOW)	[*6.25e-7* , *6.25e-6*]	0.6



[5]IAEA, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478, IAEA, Vienna (1988).

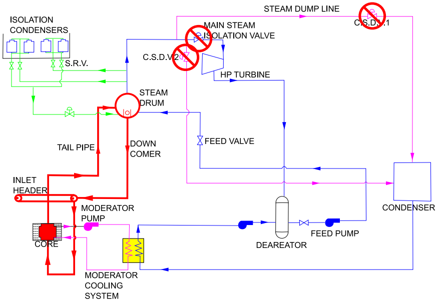
[6]Hallbert B, Kolaczkowski A. The employment of empirical data and Bayesian methods in human reliability analysis: a feasibility study. NUREG/CR-6949. Washington DC: US Nuclear Regulatory Commission; 2007.

Querying process

Time step	Evidence	MHT performance
1	$\neg D, MSIV, CSDV, IC, \neg R$	[0.959, 0.969]
2	D, $\neg MSIV, CSDV, IC, \neg R$	[0.959, 0.969]
3	D, $\neg MSIV, CSDV, IC, R$	[0.7892, 0.8192]
4	D, $\neg MSIV, CSDV, IC, R$	[0.7892, 0.8192]
$\vdots$	$\vdots$	$\vdots$
20	$\neg D, MSIV, CSDV, IC, \neg R$	[0.959, 0.969]

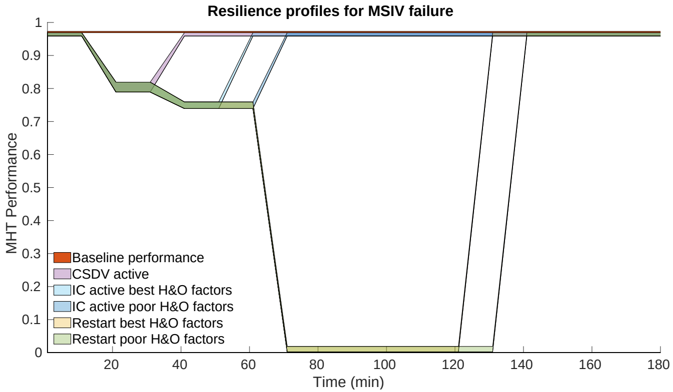
D:Disruption, R1: Restoration (good Human and Organisational conditions),

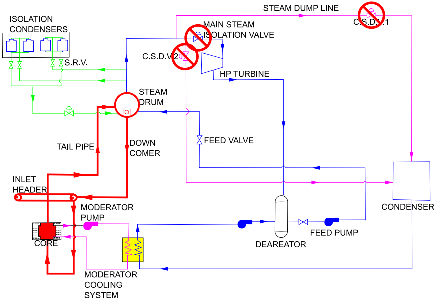
R2: Restoration (bad H&O cond.), ¬: False (or component failing).



Main Steam Isolation Valve and Condensed Steam Dump Valve out of order.

Analysis on recovery





Main Steam Isolation Valve and Condensed Steam Dump Valve out of order.

Summary

Resilience assessment with dynamic credal networks:

- Performance depends on restoration factors in disruption event.
- Component availability and organisational factors influence restoration time.
- When active components fail, restoration depends on availability of passive safety systems to control pressure in MHTS.
- Credal approach can provide confidence bounds for informed decision making.

Conclusions

Proposed methods for modelling:

- Capture complexity of system.
- Epistemic uncertainty quantification.
- Time-dependency modelling.
- Fast inference methods allow almost-real-time analysis.
- Contribution to small number of literature resources.

Analysis toolbox (available in www.cossan.co.uk):

- Allows categorisation of what-if scenarios.
- Graphical representation for ease of understanding.
- Flexibility for querying variables of interest.
- Automatic resilience profile computation.
- Open source.

Thank you for your attention

Hector Diego Estrada-Lugo
h.d.estrada-lugo@liverpool.ac.uk

Research gate: Hector_Estrada-Lugo
Linkedin: h-diego-el

Looking for postdoc position related to graphical modelling under uncertainty, thanks!

UNIVERSITY OF LIVERPOOL | Institute for Risk and Uncertainty

CONACYT Consejo Nacional de Ciencia y Tecnología