4th International Symposium on Probabilistic Methodologies for Nuclear Applications

POLITECNICO MILANO 1863

DIPARTIMENTO DI ENERGIA

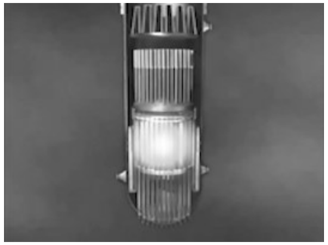
A CONDITION-BASED RISK-INFORMED DECISION-MAKING FRAMEWORK FOR SEVERE ACCIDENT MANAGEMENT

Giovanni Roma[1], Francesco Di Maio[1], Enrico Zio[1,2]

[1]Energy Department, Politecnico di Milano, Via La Masa 34, Milan 20156, Italy
[2] Mines Paris, PSL Centre de Recherche sur les Risques et les Crises, Sophie Antipolis 06904, France

Context of the work

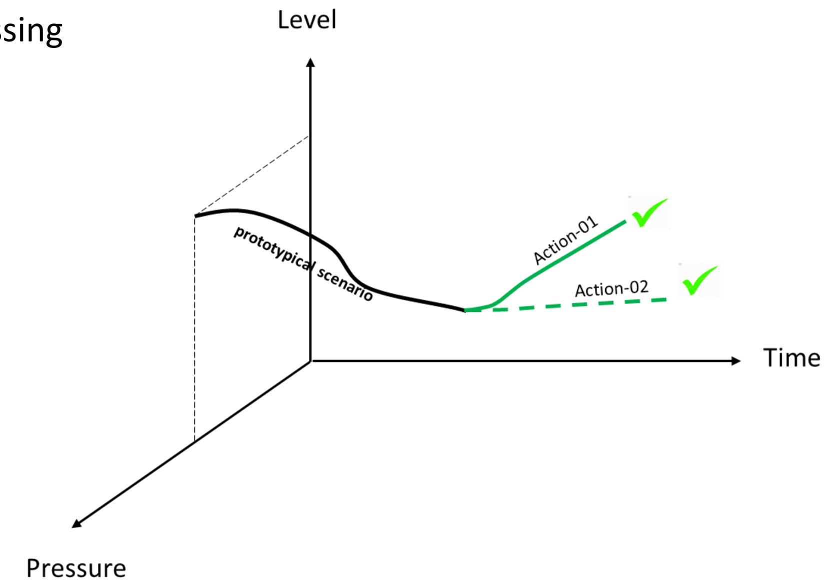
Severe Accident Management Guidelines (SAMGs) are devoted to prevent accident escalation and avoid release of radioactive materials



$$SAMG = f(Knowledge, Information, Data)$$

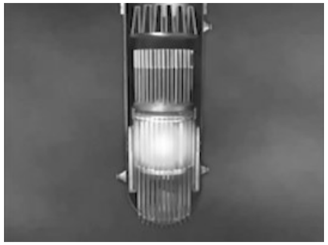
limited/missing

→ $SAMG$=f(prototypical accident scenarios)



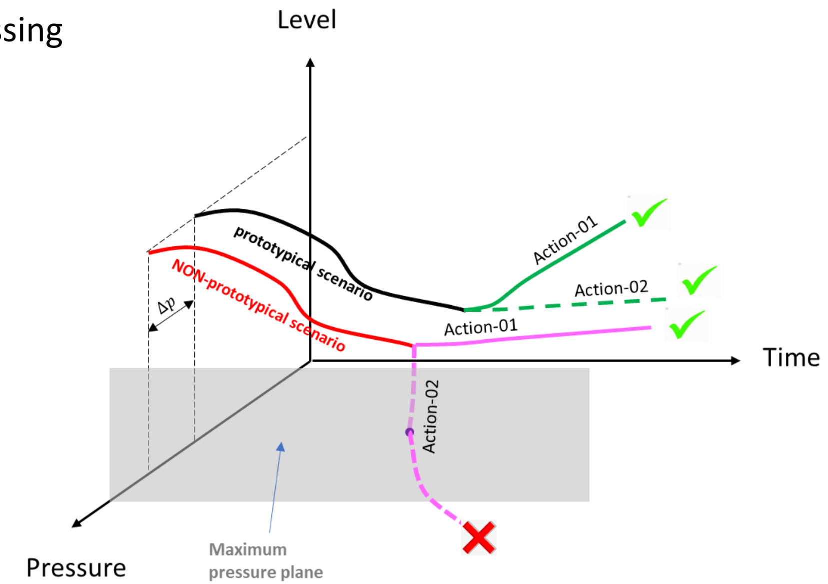
Context of the work

Severe Accident Management Guidelines (SAMGs) are devoted to prevent accident escalation and avoid release of radioactive materials



$SAMG = f(Knowledge, Information, Data)$ → $SAMG = f$(prototypical accident scenarios)

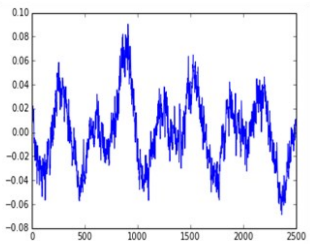
limited/missing



DIFFERENT ACTIONS HAVE DIFFERENT IMPACTS → **IS THE PROTOTYPICAL SCENARIO ENOUGH REPRESENTATIVE?**

Problem Statement

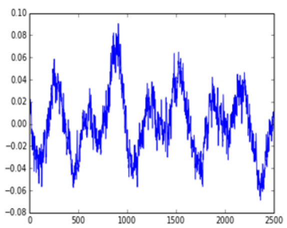
1) Plant Damage State



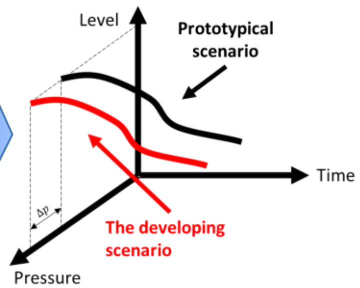
DATA FROM SENSORS

UNCERTAIN PLANT DAMAGE STATE (PDS)

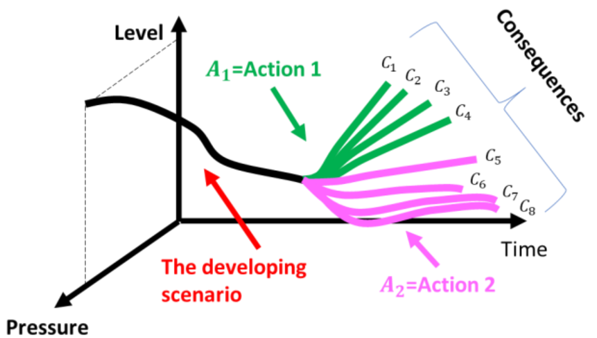
2) Developing scenario



DATA FROM SENSORS



3) Set of alternative candidate actions



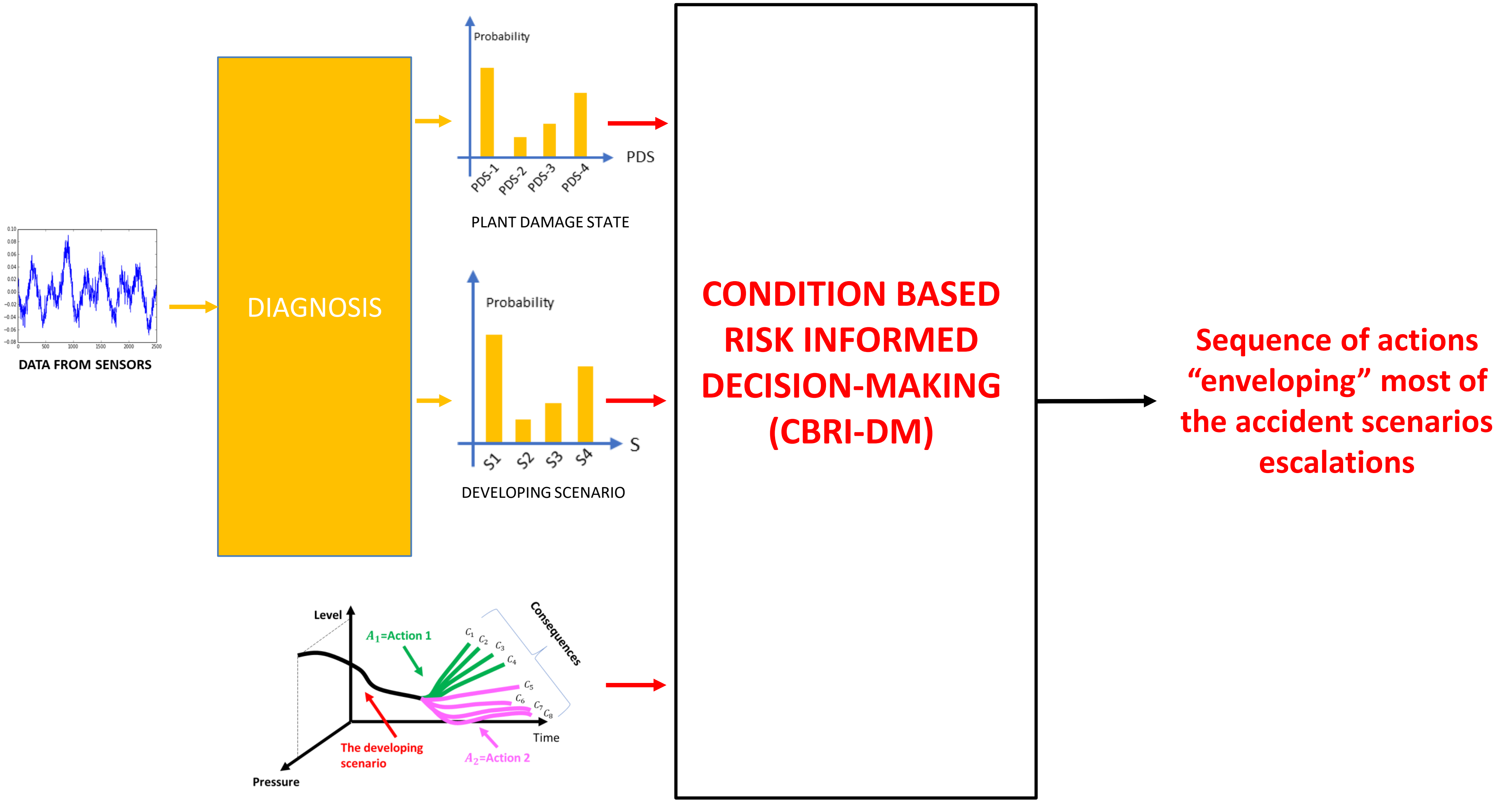
CONDITION BASED RISK INFORMED DECISION-MAKING (CBRI-DM)

→ **Sequence of actions "enveloping" most of the accident scenarios escalations**

CBRI-DM: Desiderata (1/3)

A **DIAGNOSIS MODULE** to identify:

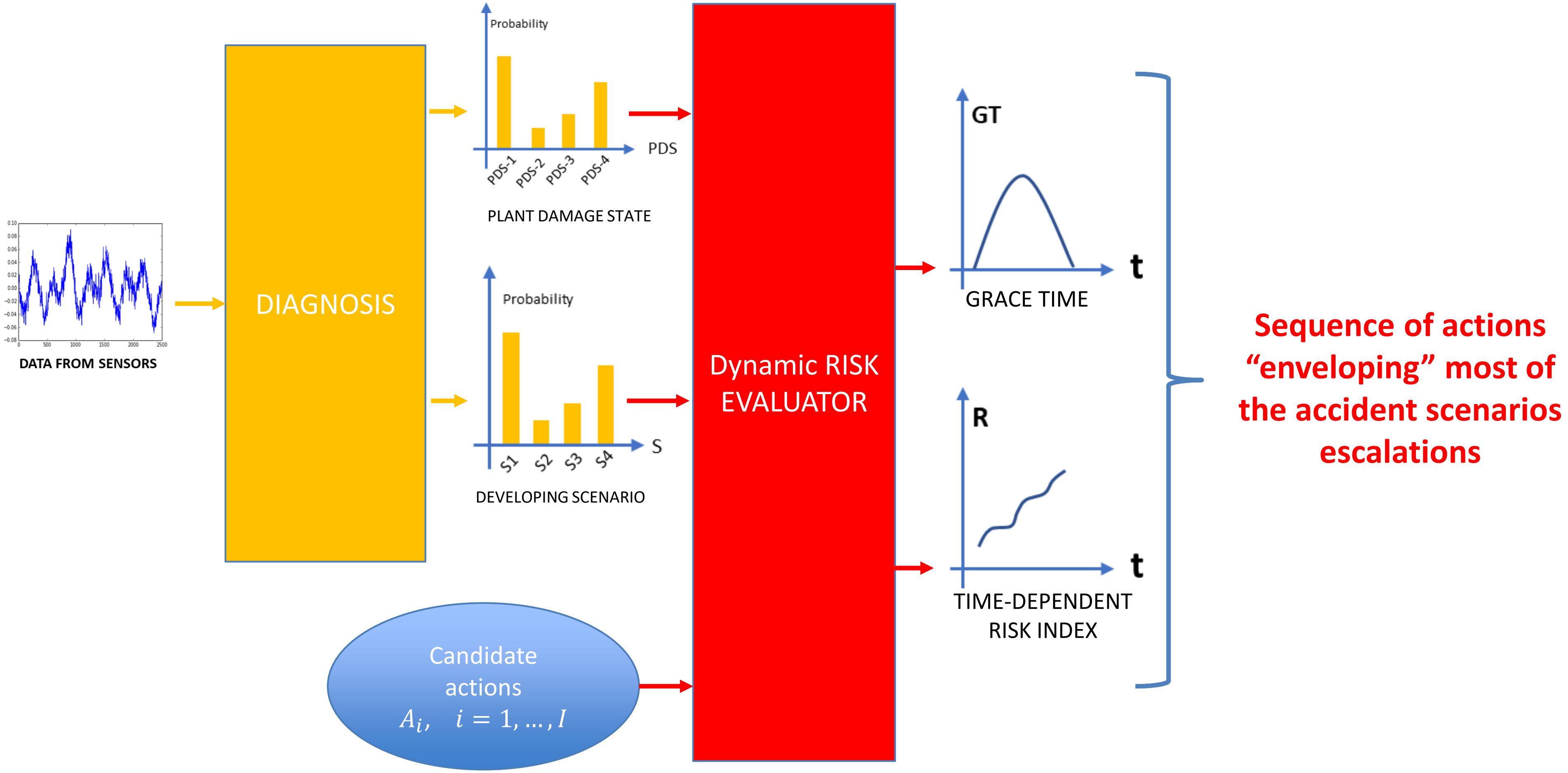
1) The Plant Damage States (PDSs) (and estimate their probability);
2) The developing scenarios (and estimate their probability).



CBRI-DM: Desiderata (2/3)

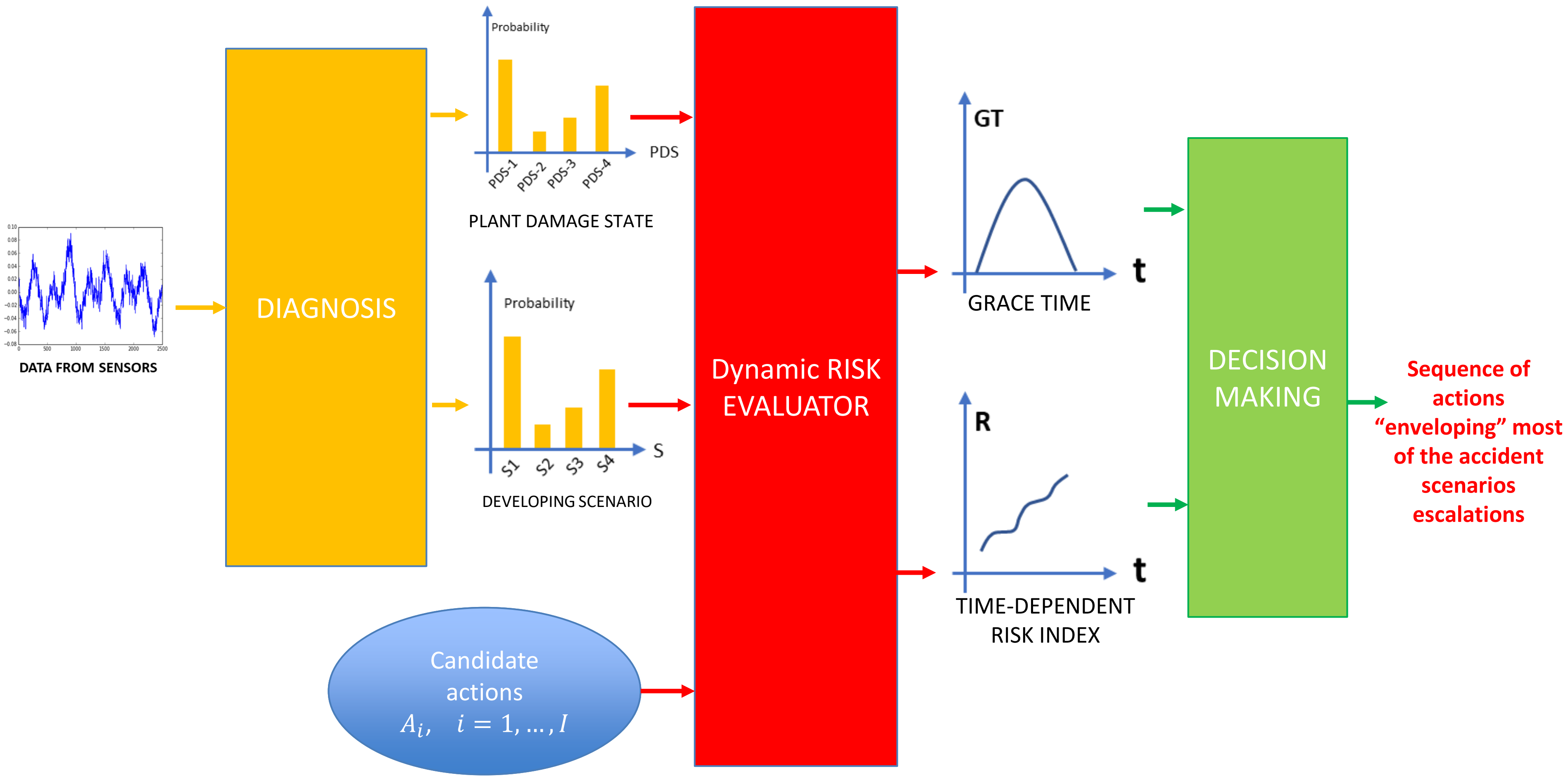
A **DYNAMIC RISK EVALUATOR** to provide:

1) The probability distribution of the Grace Time (**GT**);
2) The (time-dependent) risk index **R** @future times;

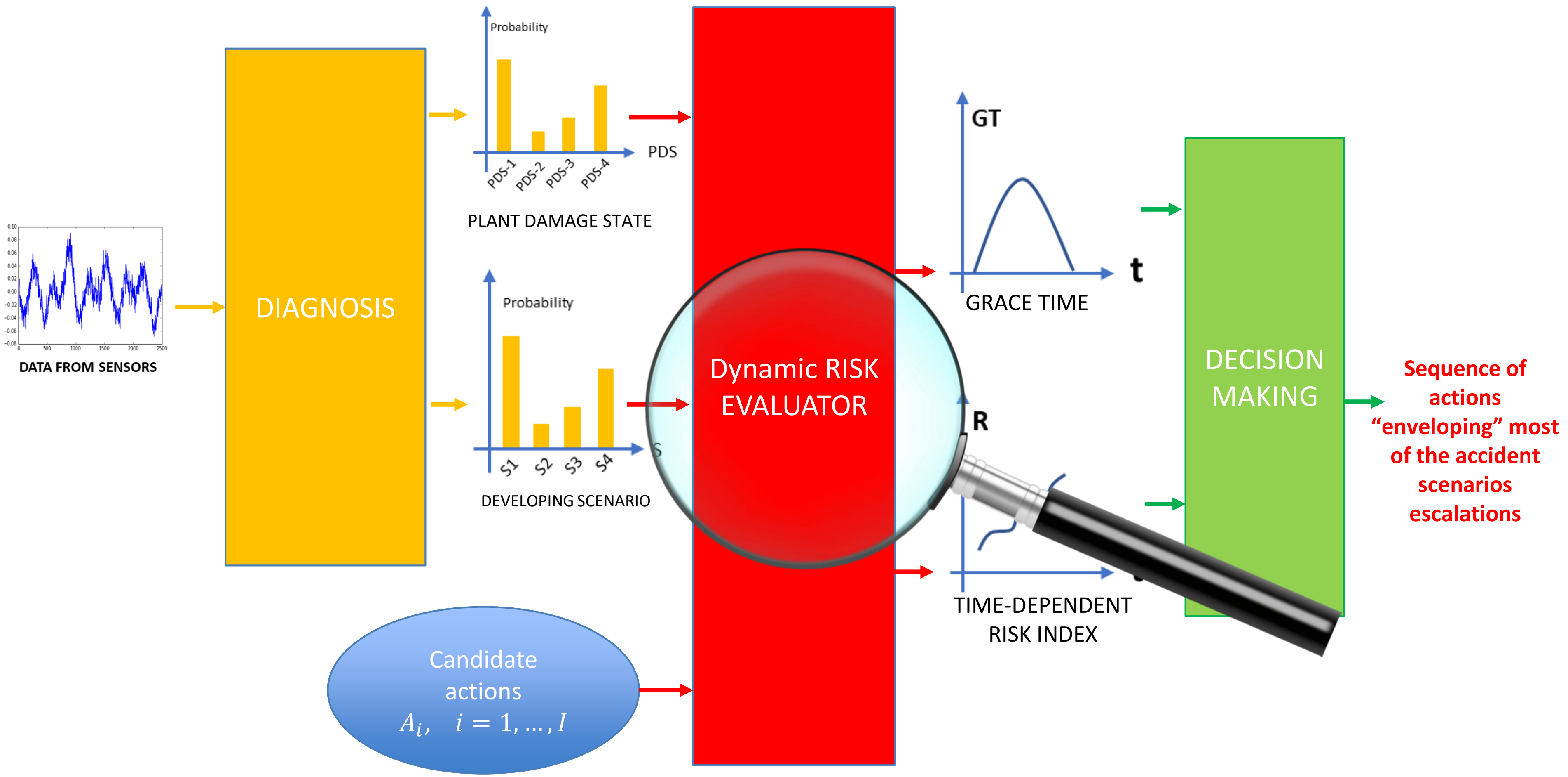


CBRI-DM: Desiderata (3/3)

A **DECISION-MAKING MODULE** to prescribe the best sequence of actions (i.e., the one "enveloping" most of the accident scenarios escalations)

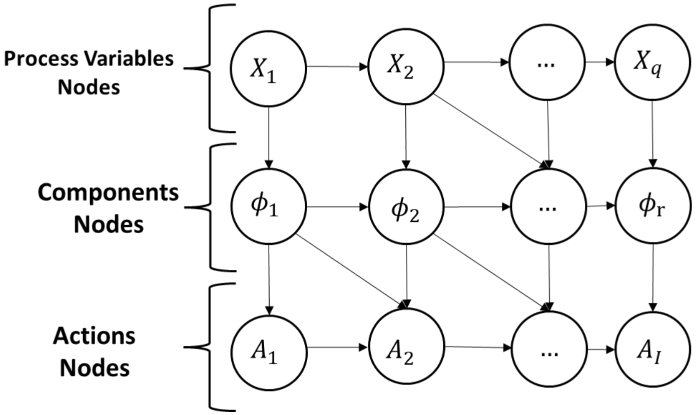


Proposed technical solution



The dynamic risk evaluator

BAYESIAN NETWORK (BN)



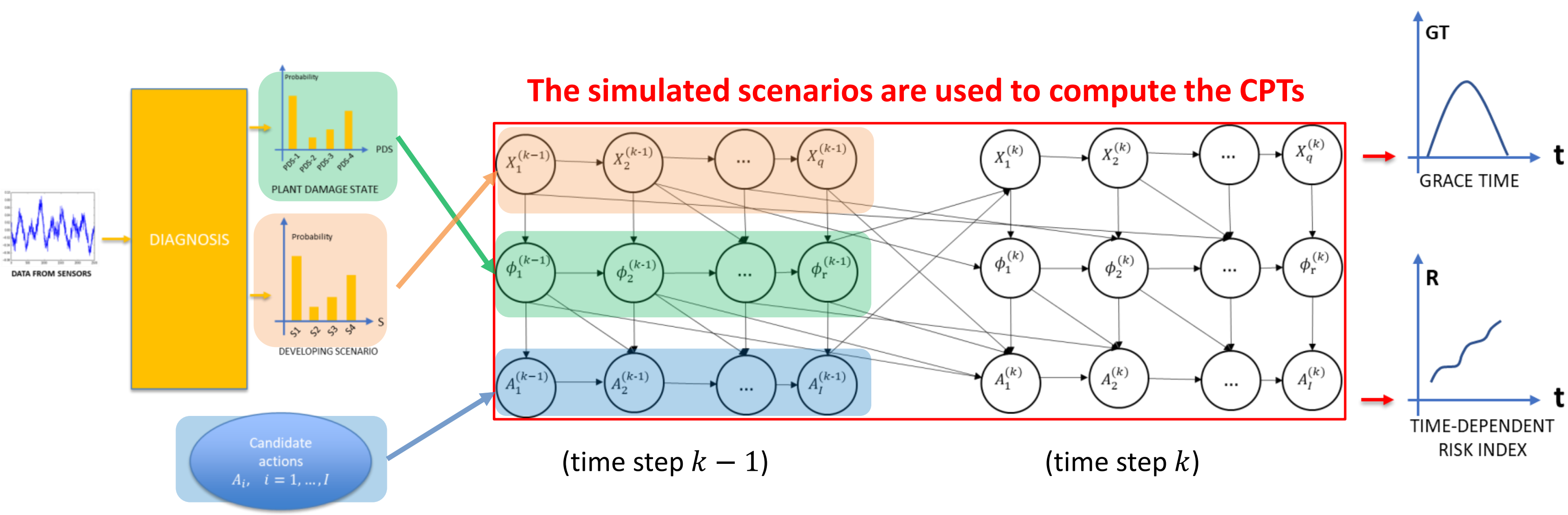
Dependencies are:

- Qualitatively represented through arrows;
- Quantitatively represented through Conditional Probability Tables (CPTs), e.g.:

	$\phi_1 = 0$		$\phi_1 = 1$	
	$X_2 = 0$	$X_2 = 1$	$X_2 = 0$	$X_2 = 1$
$\phi_2 = 0$	0,99	0,95	0,80	0,5
$\phi_2 = 1$	0,01	0,05	0,20	0,5

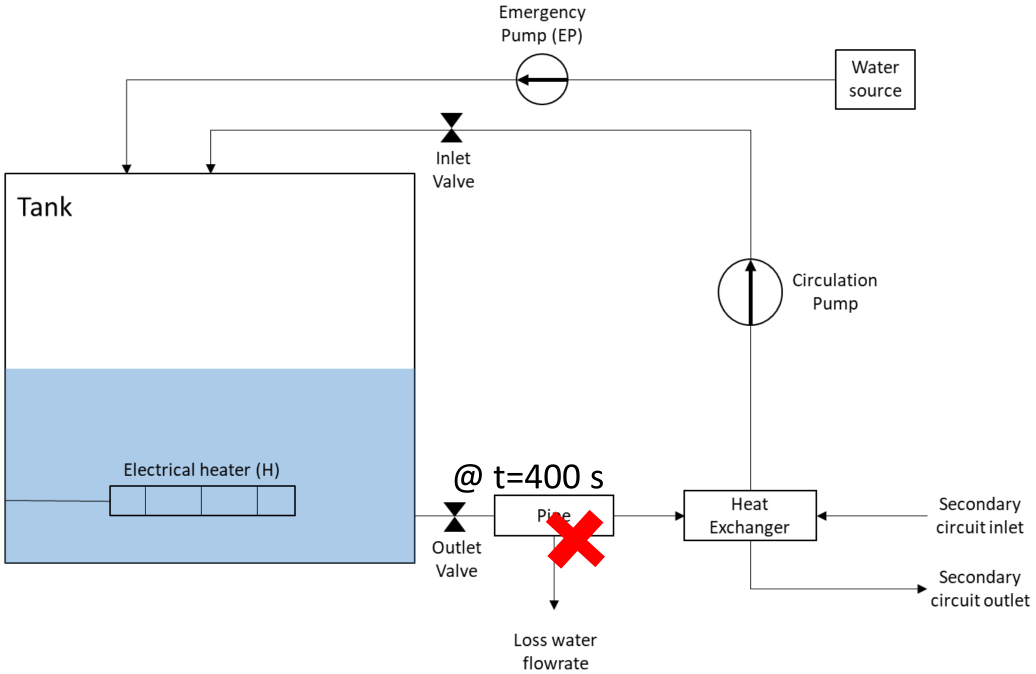
(Example of CPT for binary nodes)

DYNAMIC BAYESIAN NETWORK (DBN)



Case study (1/2)

- **System:** Electric Heating System [6] ;
- **Model:** Simulink;
- **System goals**:
  - Water Level $(L) > 2\ m$;
  - Water Temperature $(T) < 80\ °C$;
- **Transient time**: $t = [0s, 1000s]$;



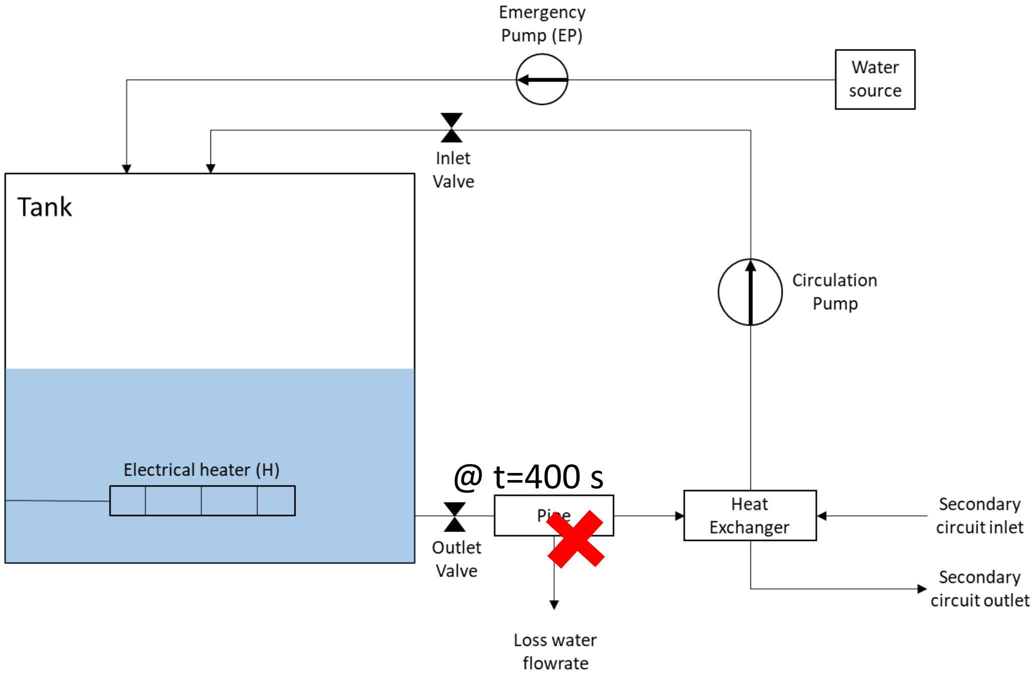
- **Assumptions:**
  - The EP and the H cannot be simultaneously switched ON and OFF, respectively;
  - The heater H and the EP have two possible operational status (i.e., ON-OFF);
  - Once the heater become OFF it will not become ON again;
  - No running failure for the EP.

EP= Emergency Pump;
H= Electrical Heater;

Case study (2/2)

- **Accidental Scenarios characteristics:**

- Primary circuit pipe rupture @ t=400 s;
- Random variables for scenarios generation:
  1. Fraction of loss flowrate:
     Uniform $U[0.05, 0.10]$;
  2. Type of operating option:
     Uniform U[turn on the EP first, turn off the H first];
  3. Time to turn ON the Emergency Pump (EP):
     Uniform $U\ [100\ s, 350s]$;
  4. Time to turn OFF the Heater (H):
     Uniform $U\ [100\ s, 350s]$

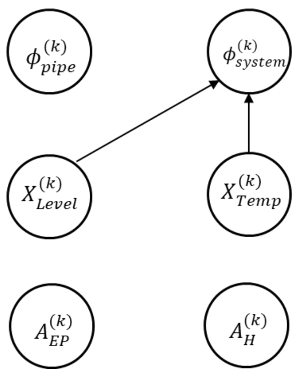


Four actions are compared:

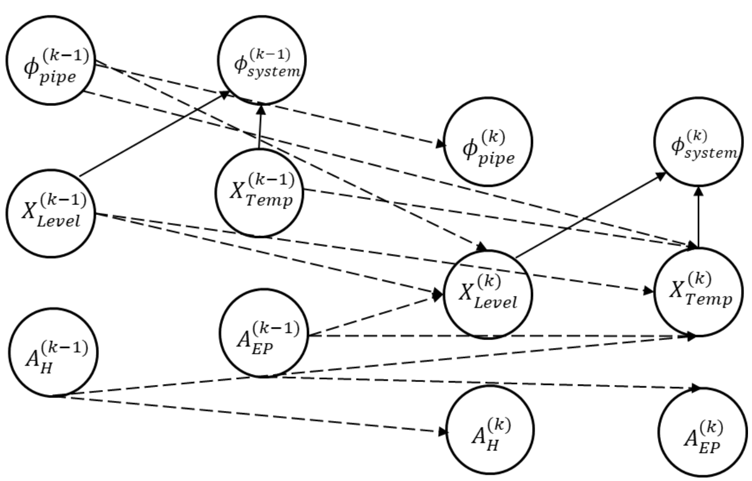
- $A_1 = (EP = on\ @t = 500s, \mathrm{H} = \mathrm{off}\ @\mathrm{t} = 600\mathrm{s})$;
- $A_2 = (EP = on\ @t = 600s, \mathrm{H} = \mathrm{off}\ @\mathrm{t} = 500\mathrm{s})$;
- $A_3 = (EP = on\ @t = 500s, \mathrm{H} = \mathrm{off}\ @\mathrm{t} = 700\mathrm{s})$;
- $A_4 = (EP = on\ @t = 700s, \mathrm{H} = \mathrm{off}\ @\mathrm{t} = 500)$;

The DBN

The BN of the system



The DBN of the system



$\Delta t = 50\ s$ → k=(0,1,...,21)

System nodes are discretized

Pipe_state	
State	Description
TRUE	Pipe failed
FALSE	Pipe working

Sys_state	
State	Description
TRUE	System failed
FALSE	System working

Water Level (L)	
State	Description
L1	L < 2m
L2	2m < L< 3m
L3	3m < L < 4m
L4	L > 4m

Temperature (T)	
State	Description
T1	T < 20°C
T2	20°C < T< 40°C
T3	40°C < T< 60°C
T4	60°C < T< 80°C
T5	T>80°C

Heater (H)	
State	Description
ON	H on
OFF	H off

Emergency Pump (EP)	
State	Description
ON	EP on
OFF	EP off

Monte Carlo Simulations are performed to compute the CPTs

Case study: Results (1/2)

System state @t=450s:

- $X_L^{(9)} = \mathrm{L3};$
- $X_T^{(9)} = T4;$

Action – 1:

- Turn On EP @ t=500s;
- Turn off H @ t=600s;

Action – 2:

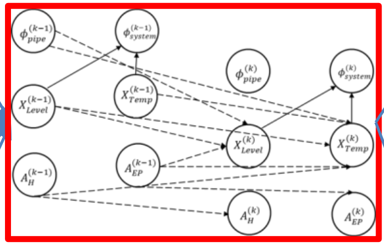
- Turn On EP @ t=600s;
- Turn off H @ t=500s;

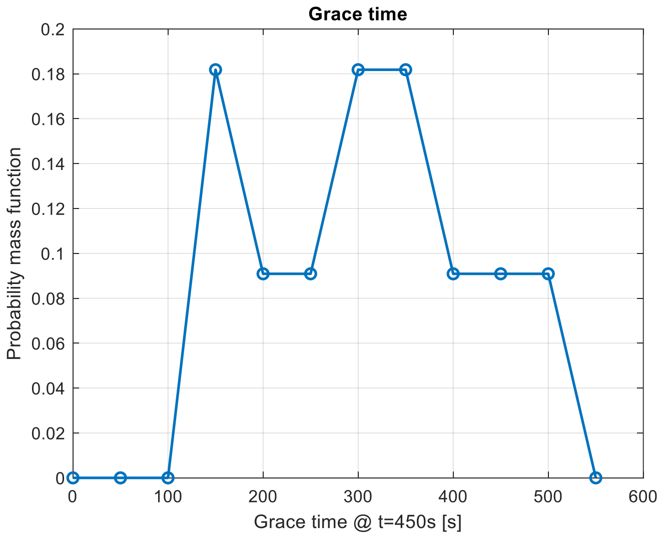
Action – 3:

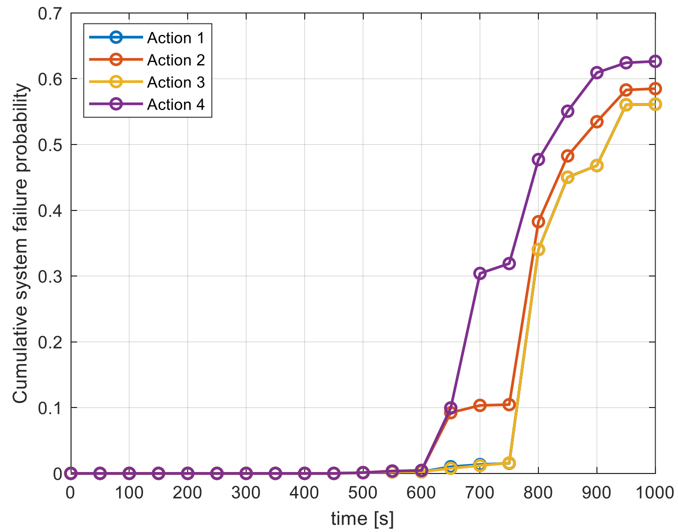
- Turn On EP @ t=500s;
- Turn off H @ t=700s;

Action – 4:

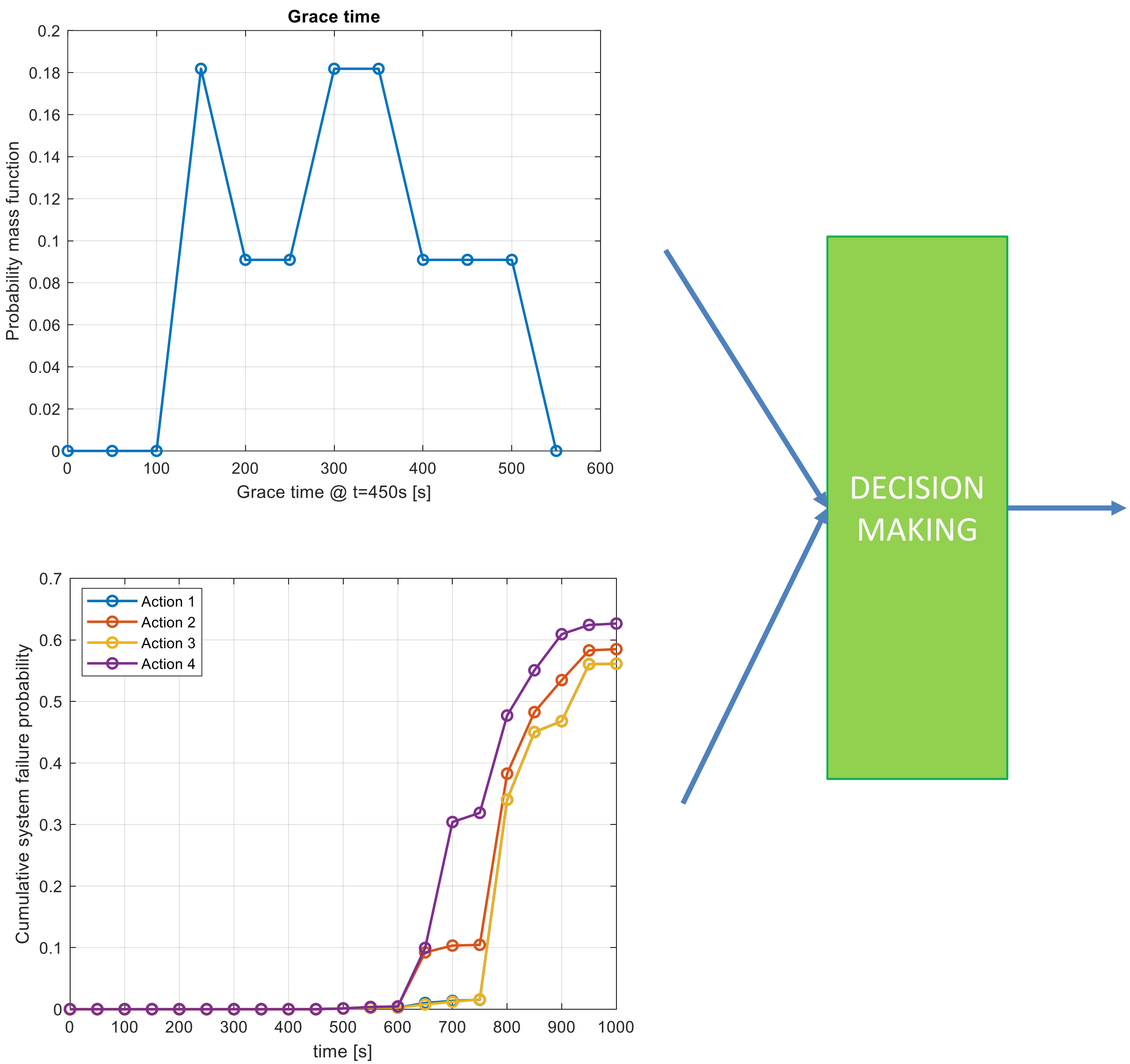
- Turn On EP @ t=700s;
- Turn off H @ t=500s;







Case study: Results (2/2)



Action 1 and Action 3 are those "enveloping" most of the accident scenarios escalations

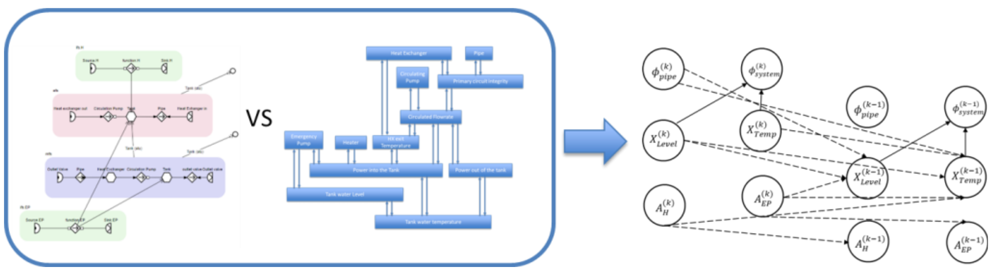
Conclusions and future works

1. **A framework based on DBNs for combining condition-monitoring data with dynamic risk assessment has been proposed for decision-making in support of SAMGs;**

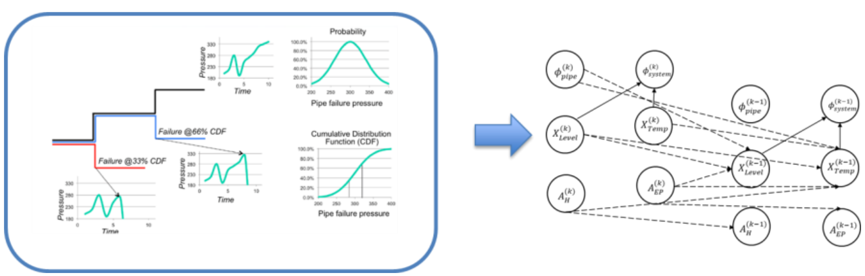
2. **The feasibility of application of the proposed framework has been shown on a case study;**

3. **Technical issues for the informed construction of the DBN need to be addressed with respect to the opportunity of using:**

   a) Multilevel Flow Modelling (MFM) or System Theoretic Accident Model and Processes (STAMP) **to model the interdependencies in the system**;



   b) Dynamic PRA methodologies for a **comprehensive coverage of accidental scenarios for the inference of CPTs**;



   c) Hybrid Bayesian Network to **avoid parameters discretization**.

References

1) Jaewhan Kim, Jaehyun Cho. Technical challenges in modeling human and organizational actions under severe accident conditions for Level 2 PSA. Reliability Engineering & System Safety, Volume 194, February 2020, 106239.
2) IAEA. Implementation of Accident Management Programmes in Nuclear Power Plants - Safety Reports Series No. 32 2004:129.
3) NEA. Informing Severe Accident Management Guidance and Actions for Nuclear Power Plants through Analytical Simulation, NEA/CSNI/R(2017)16. Organ Econ Co-Operation Dev 2018.
4) Mahdi Saghafi, Mohammad B. Ghofrani. Accident management support tools in nuclear power plants: A post-Fukushima reviewProgress in Nuclear Energy 92 (2016) 1-14.
5) Weber P, Jouffe L. Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)☆☆Revised version of the paper presented at QUALITA 2003. Reliab Eng Syst Saf 2006;91:149–62. https://doi.org/https://doi.org/10.1016/j.ress.2005.03.006.
6) J. Kim et al. System risk quantification and decision making support using functional modeling and dynamic Bayesian network. Reliability Engineering and System Safety 215 (2021) 107880.
7) MORTEN LIND and XINXIN ZHANG. FUNCTIONAL MODELLING FOR FAULT DIAGNOSIS AND ITS APPLICATION FOR NPP. Nuclear engineering and technology. Volume 46, Issue 6, December 2014, Pages 753-772.
8) NANCY G. LEVESON, JOHN P. THOMAS. STPA handbook. MARCH 2018.
9) Salmerón A, Rumí R, Langseth H, Nielsen TD, Madsen AL. A review of inference algorithms for hybrid Bayesian networks. J Artif Intell Res 2018;62:799–828. https://doi.org/10.1613/jair.1.11228.
10) Tunc Aldemir. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy 52 (2013) 113–124.

Thank you for your attention!

Appendix 1: Identifying interdependencies within the system (1/3)

ISSUE

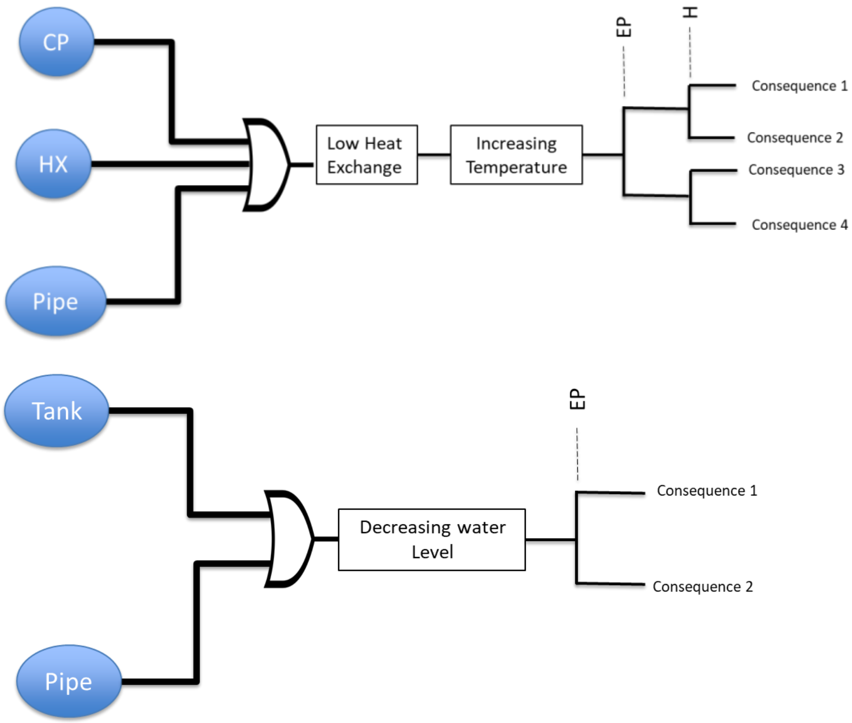
Classical approaches:

- Fault Tree;
- Event Tree;
- Bow-Tie

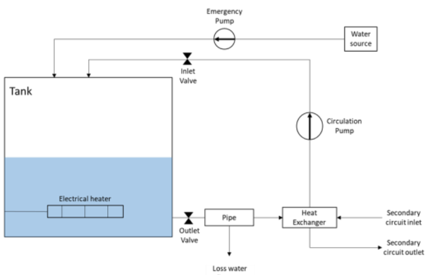
Used to find relations between system's states/events.

No explicit representation of system/component's functions and objectives.

EXAMPLE



Legend:
CP= Circulation Pump;
HX= Heat Exchanger;
EP= Emergency Pump;
H= Heater



PROPOSED SOLUTIONS

Two **alternatives:**

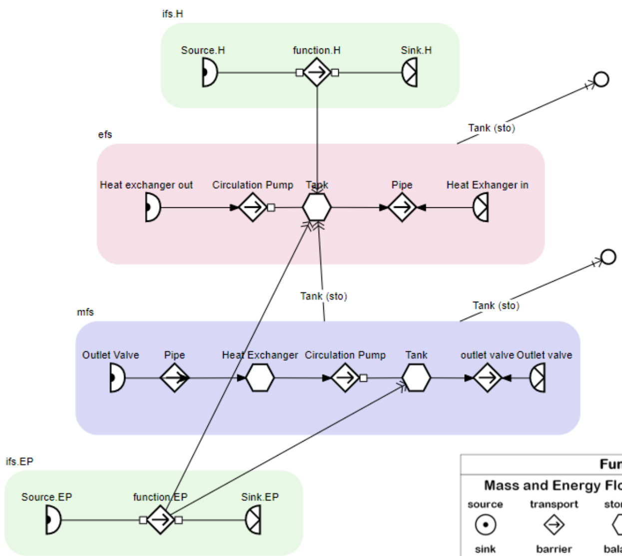
A. Multilevel Flow Modeling (MFM);

B. System Theoretic Accident Model and Processes (STAMP)

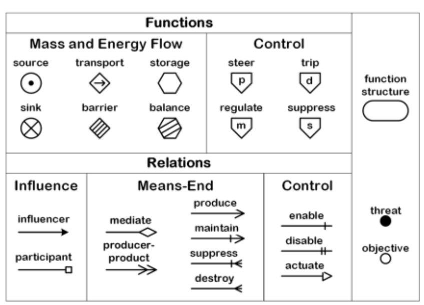
Appendix 1: Identifying interdependencies within the system (2/3)

Multilevel Flow Modelling [7]

1) Representation of the system's:
   - Goals;
   - Functions to reach the goals;
   - The relationships and interactions between them.
2) Hierarchical decomposition of the system in sub-systems and components.

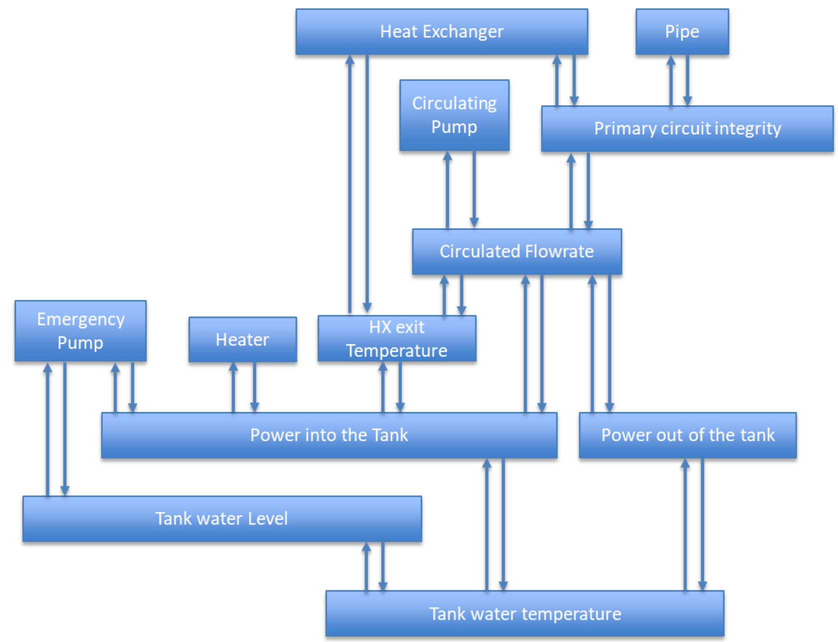


Legend



System Theoretic Accident Model and Processes [8]

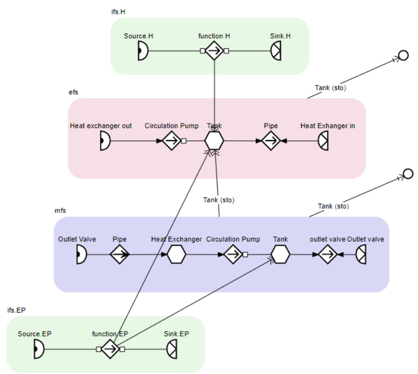
1) Representation of the system in terms of:
   - Controllers;
   - Controlled processes/variable;
   - The relationships and interactions between them (in terms of control actions and feedback).
2) Hierarchical decomposition of the system in sub-systems, components and processes.

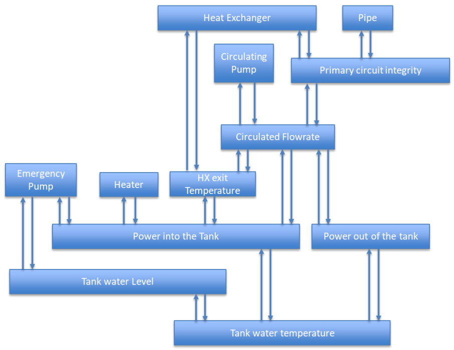


Appendix 1: Identifying interdependencies within the system (3/3)

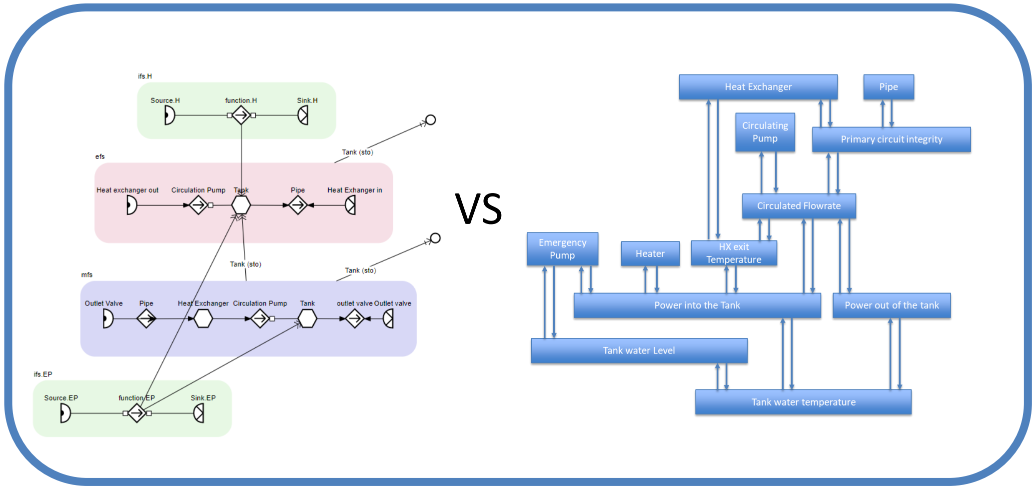
Steps to build the structure of DBN:

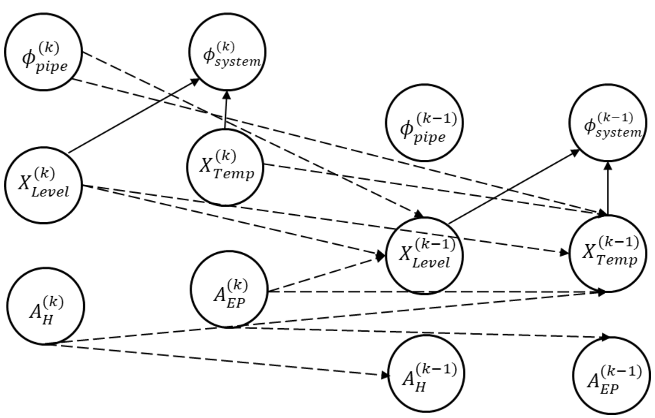
1. Identify interdependencies within the system through MFM or STAMP:





2. Map the MFM or the STAMP control structure into a DBN:





Appendix 2: Coverage of accidental scenarios for the inference of CPTs (1/2)

ISSUE

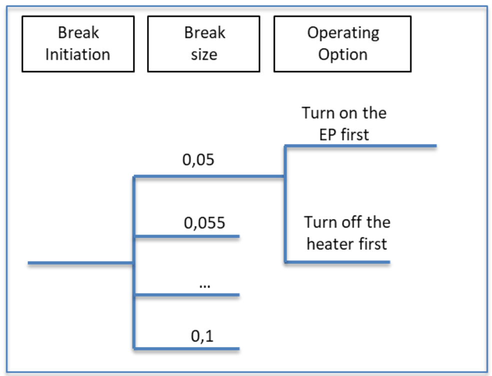
Classical approach:

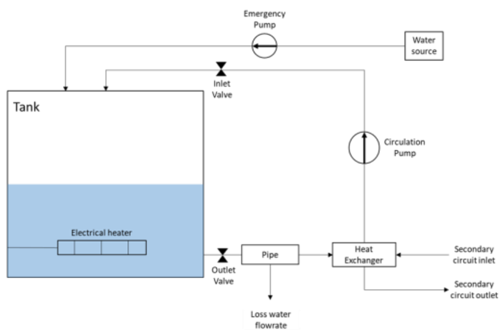
- Event Tree (ET);

Used to generate accidental scenarios.

- Timing of events not taken explicitly into account
- ET headers a priori chosen

EXAMPLE

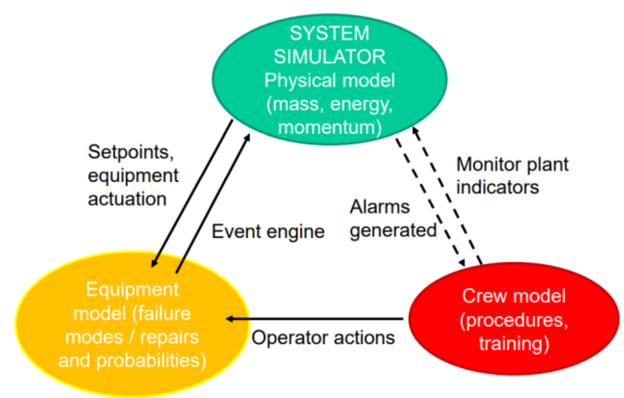




PROPOSED SOLUTION

Dynamic PRA Methodologies (e.g., DET)

- Integration of deterministic (i.e., simulator) and stochastic processes (i.e., degradation and failure event occurrences)
- Explicit modelling of the plant-crew interactions.



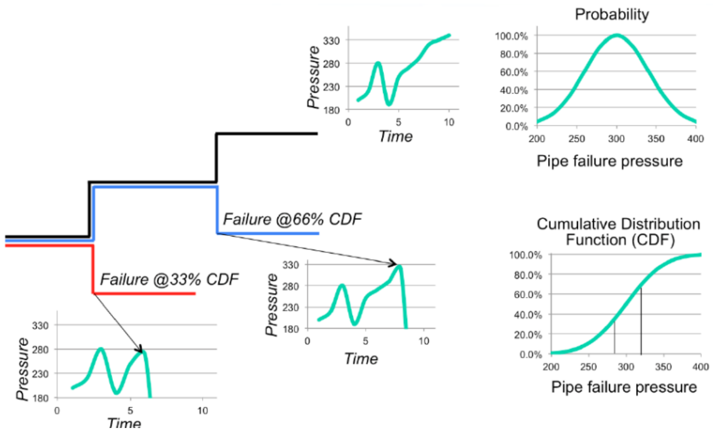
Appendix 2: Coverage of accidental scenarios for the inference of CPTs (2/2)

DET logic

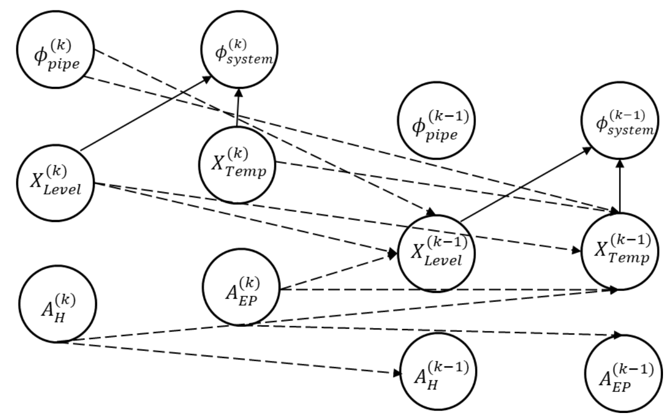
- Events in the system occur at specified branching points according to the branching rules;
- Branching rules are specified by users (through PDFs);
- According to these rules, the simulation spoons different branches
- For each spoon, the system is simulated until another event occurs and a new set of branching is spooned;
- The simulation ends when an exit condition or a maximum mission time is reached.

Advantages

- Timing of events is explicitly considered;
- Identification of accident scenarios which may have been overlooked by the analyst in the (static) PRA analysis;
- Time-dependent PDFs of components and process variables can be found;



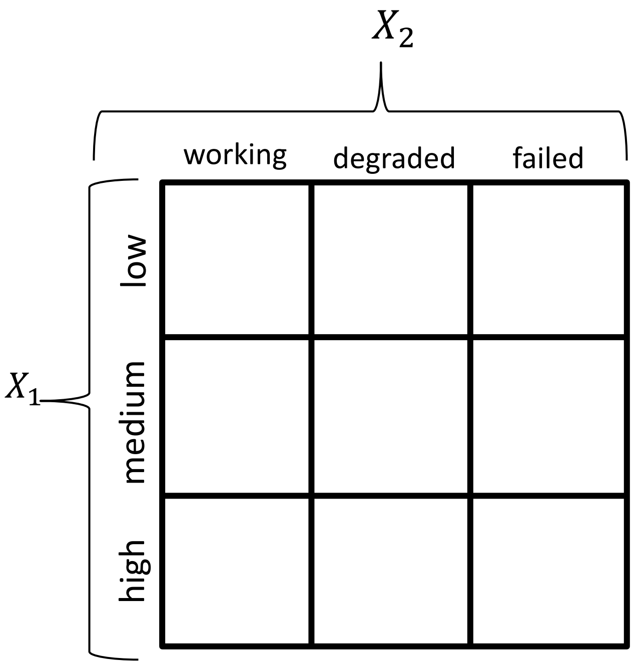
Rabiti, Cristian et al. "HYBRID DYNAMIC EVENT TREE SAMPLING STRATEGY IN RAVEN CODE A.Alfonsi**,." (2014).



Appendix 3: Discretization of nodes' states

ISSUE

Node Discretization



TECHNICAL SOLUTION

Hybrid Dynamic Bayesian Networks [9]

ADVANTAGES

1. **No need to discretize critical parameters (which may impact on the reliability assessment);**
2. **Continuous and discrete variables (nodes) handled simultaneously.**

DRAWBACK

- **Higher computational cost;**
- **Need to explore suitable inference algorithms.**

Appendix 4: The Integrated Framework