Modelling of Nuclear Systems for Resilience Assessment

T.V. Santhosh, Edoardo Patelli
Institute for Risk and Uncertainty
University of Liverpool, UK

UNIVERSITY OF LIVERPOOL
University of Strathclyde
EPSRC
Engineering and Physical Sciences Research Council

Contents

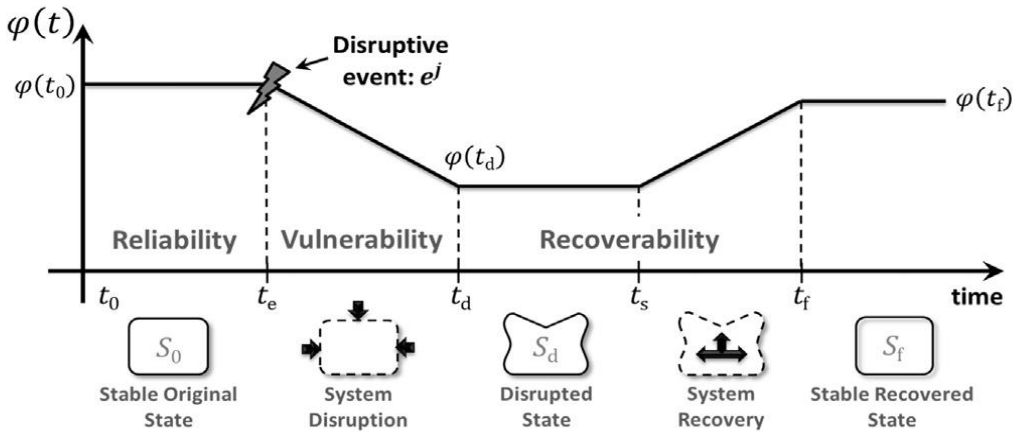
Resilience engineering

- Resilience engineering is a concept that can increase the reliability and safety level in high risk environments *such as petrochemical plants, NPP, etc.*

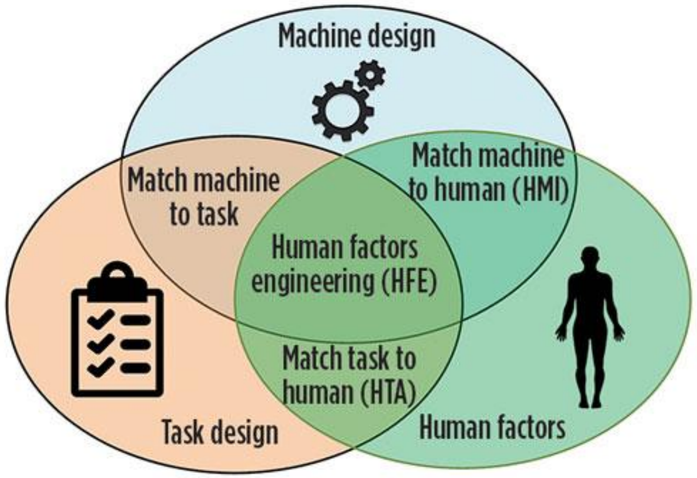
- The goal of RE is not to avoid the occurrence of threats but to manage them in a more efficient manner

- RE focuses on action to compensate for poor behavior, poor design, poor systems, and poor conditions

- Performance evaluation of human resources in most systems is an issue of paramount importance for managers, researchers, and decision-makers



S_0: Stable original state
S_d: Disrupted state
S_f: Stable recovered state



Type A: Errors made during normal operation prior to any transient (initiating event)

- These include typically periodic testing, calibrations, preventive maintenance, shift works and equipment isolations.

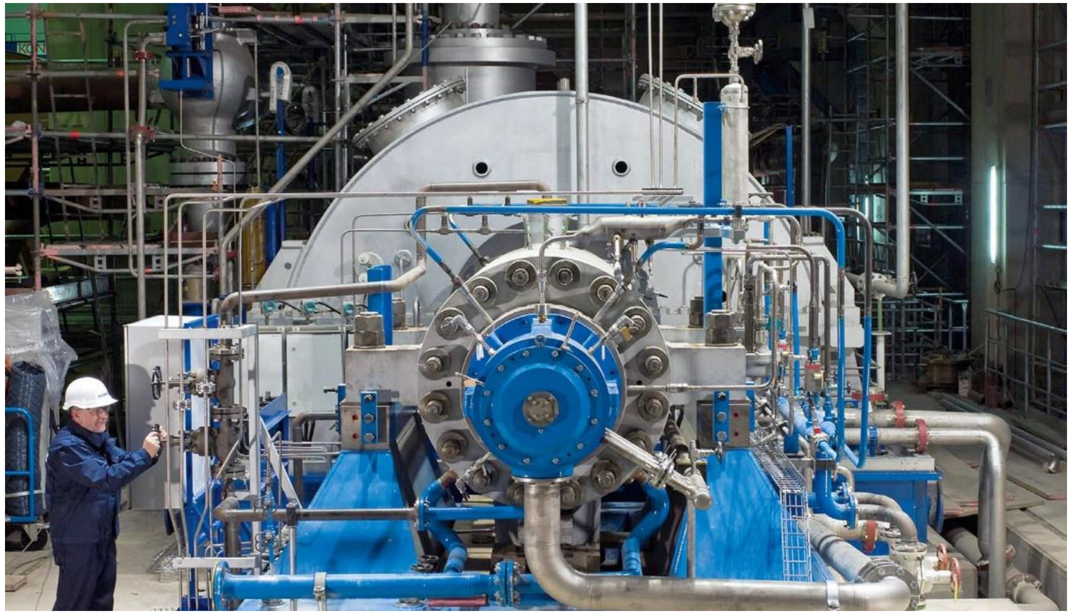
Type B: Errors and actions that cause an initiating event

- Accident initiating interactions during normal operation and maintenance

Type C: Errors made after an initiating event

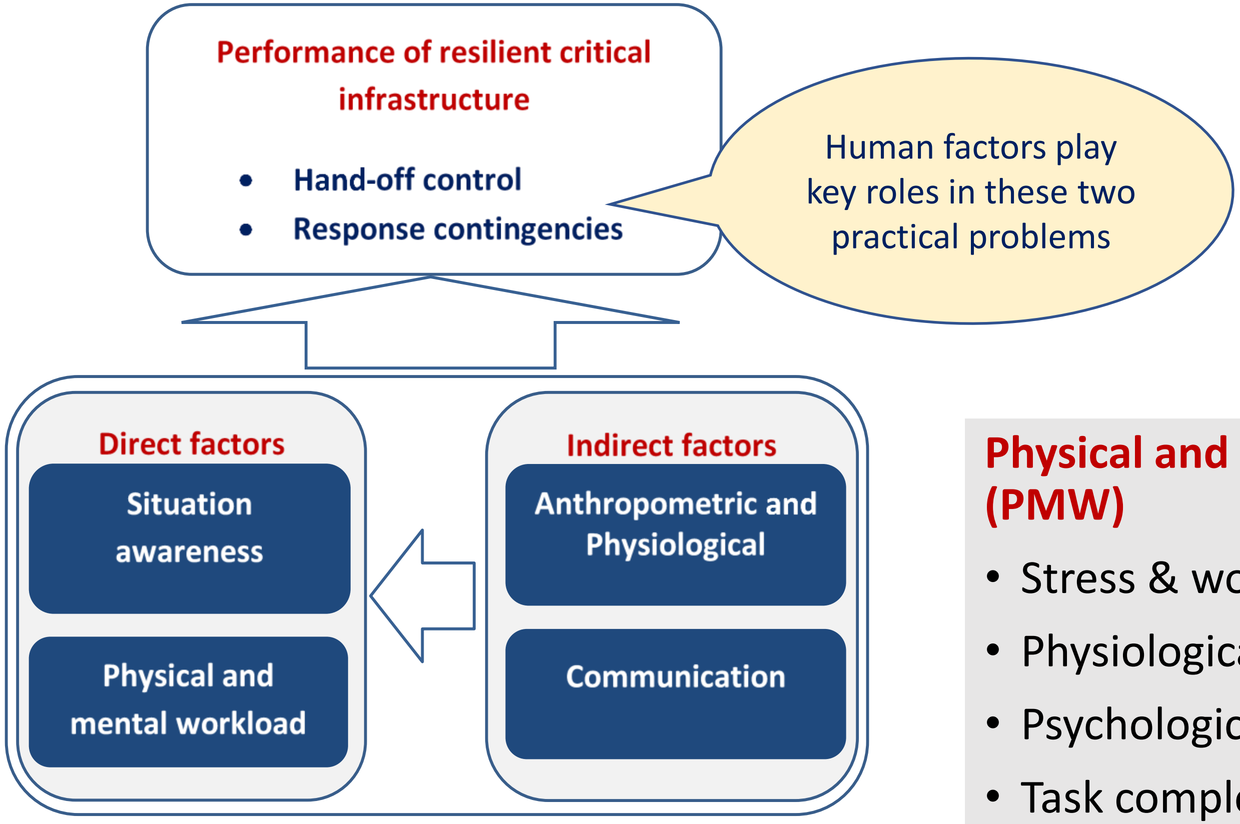
- These occur during actions intended to activate a safety function or to use an alternative system, and possible errors made in trying to recover in time from a dangerous situation.

- **Main causes of human error**
  - Procedure violation
  - Procedure content
  - Procedure format
  - Work organization
  - Task complexity
  - Inadequate training
  - Workload factors
  - Work station design



- **Types of human error**
  - Slip – Correct intention, failed execution
  - Mistake – Misinterprets situation, incorrect plan of action
  - Lapse – Forgetting action

Factors influencing the performance of critical infrastructure



Physical and Mental Workload (PMW)

- Stress & workload
- Physiological state
- Psychological state
- Task complexity
- Abilities
- Training and Experience
- Team factors (communication)

Situation Awareness (SA)

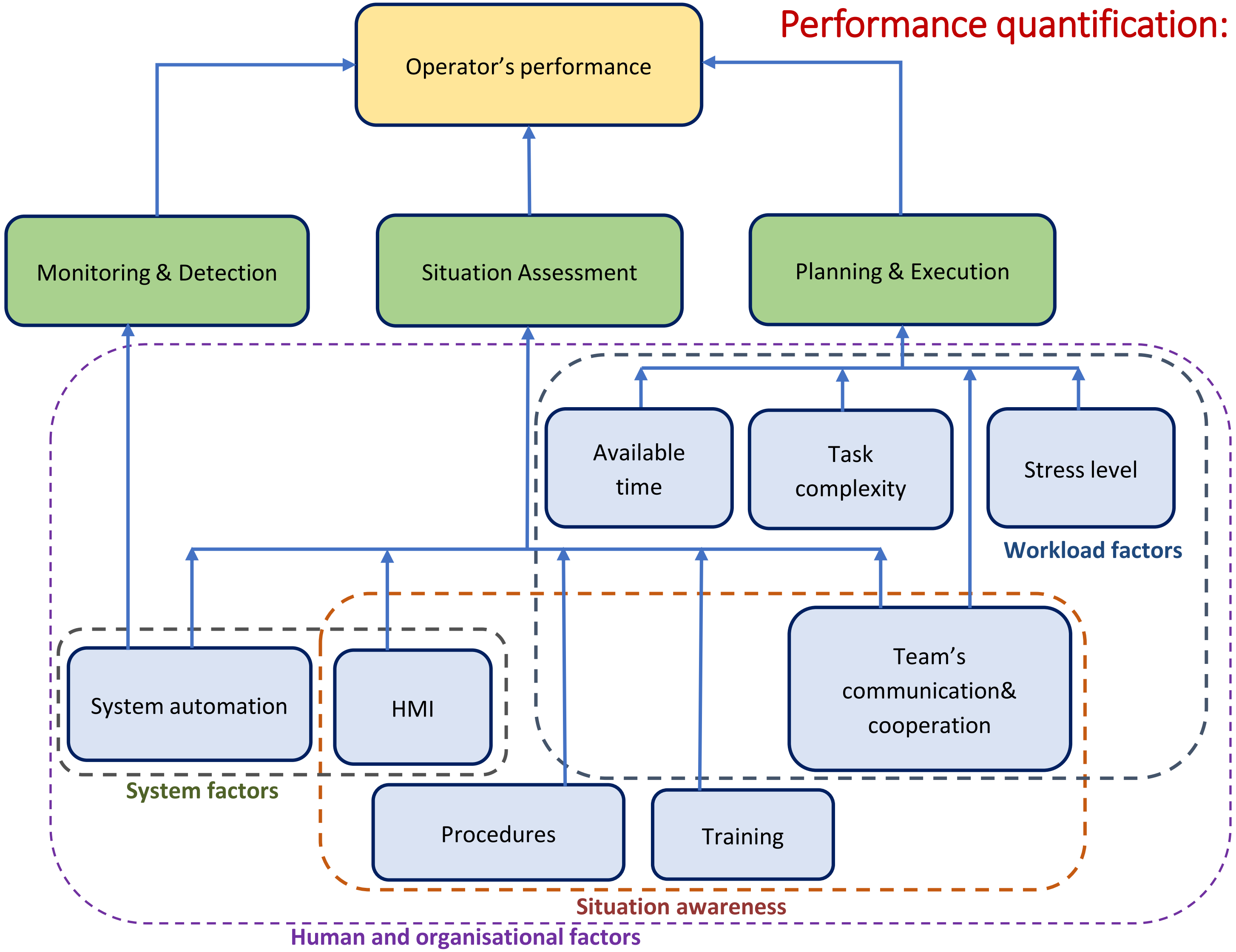
Individual factors

- Abilities
- Training and Experience

System/task factors

- System flexibility
- Human Machine Interface (HMI)
- Automation
- Procedures
- Task complexity
- Available time
- Team factors (communication)

Factors influencing the performance of operator



Performance quantification: THERP, ASEP, HEART, CREAM, ATHENA, HCR, SPAR-H

PSF	PSF Level	P(PSF)
Available Time	Expansive time	0.023
	Extra time	0.136
	Nominal time	0.683
	Barely Adequate time	0.159
	Inadequate time	1.0E-6
Stressors	Nominal	0.841
	High	0.136
	Extreme	0.023
Complexity	Nominal	0.5
	Moderately complex	0.341
	Highly complex	0.159
Experience/Training	High	0.333
	Nominal	0.333
	Low	0.333
Procedures	Nominal	0.450
	Available, but poor	0.3
	Incomplete	0.2
	Not available	0.05
HMI	Good	0.159
	Nominal	0.683
	Poor	0.136
	Missing/Misleading	0.023
Fitness for duty	Nominal	0.841
	Degraded fitness	0.159
	Unfit	1.0E-6
Work processes	Good	0.159
	Nominal	0.819
	Poor	0.023

Human Cognitive Reliability (HCR) Model (NUREG-1278F)

$$P(t) = e^{-\left[\frac{\frac{t}{T'_{\frac{1}{2}}} - Bi}{Ai}\right]^{Ci}}$$

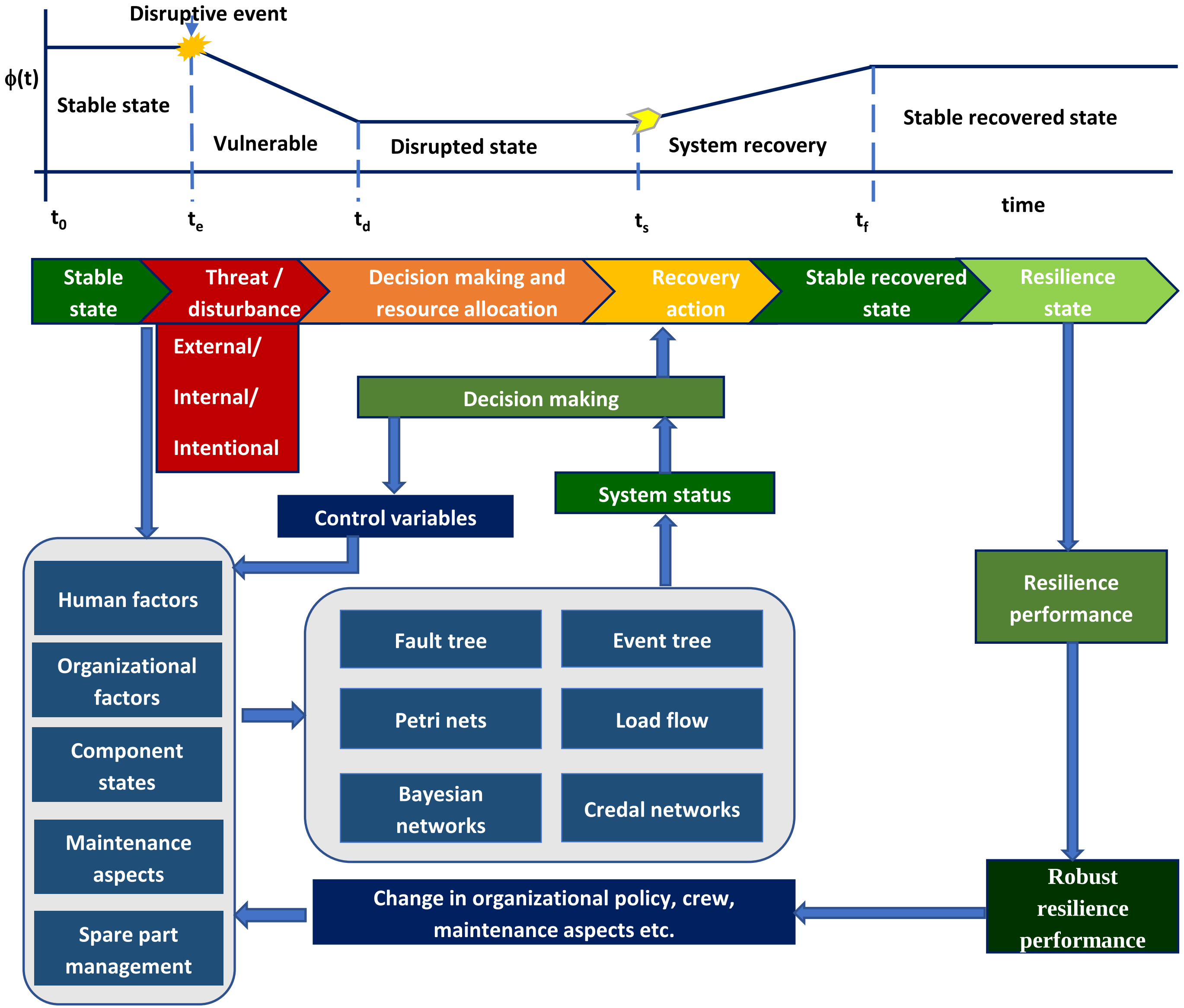
Cognitive Processing Type	Ai	Bi	Ci
Skill	0.407	0.7	1.2
Rule	0.601	0.6	0.9
Knowledge	0.791	0.5	0.8

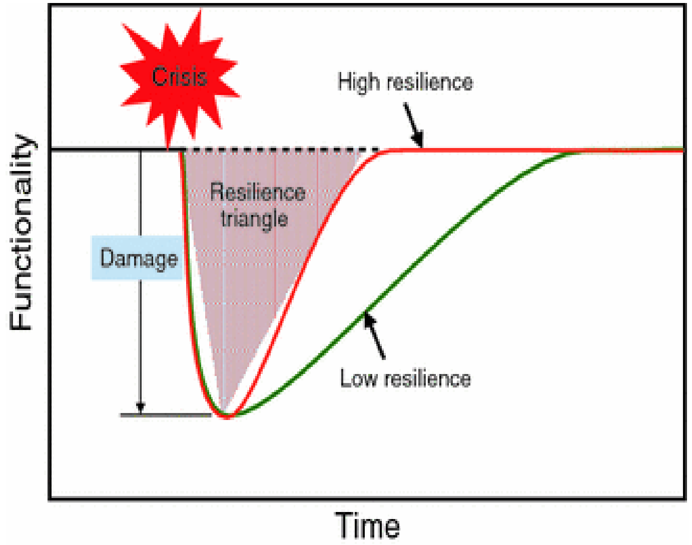
- t= time available to complete the action or set of actions following an event
- $T'_{1/2}$ = estimated median time to complete the task (action or set of actions) as adjusted by specific PSFs.

$$T'_{\frac{1}{2}} = T_{\frac{1}{2}}(1 + k1)(1 + k2)(1 + k3)$$

- Where, k1, k2 and k3 are the PSF coefficients for Experience, Stress and MMI.
- The probability distribution of crew’s response to event depends on the behavior involved (skill, rule or knowledge).

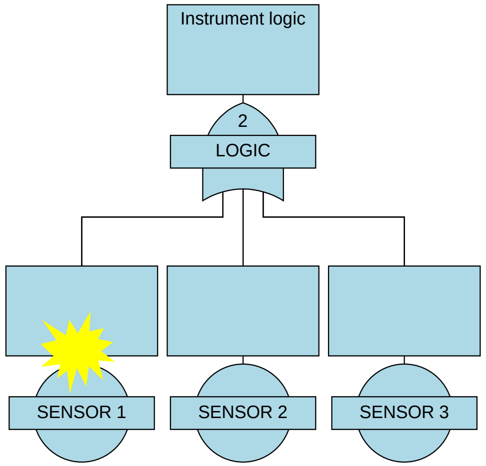
Framework for resilience assessment of critical infrastructure





Case study: Unexpected threat on regulating system of thermal reactor

- **Regulating system**
  - 4 regulating rods
    - Regulating rods are used for regulation of power
  - 4 shim rods
    - Shim rods are used for reactor setback
  - 8 absorber rods
    - Absorber rods are used for xenon override

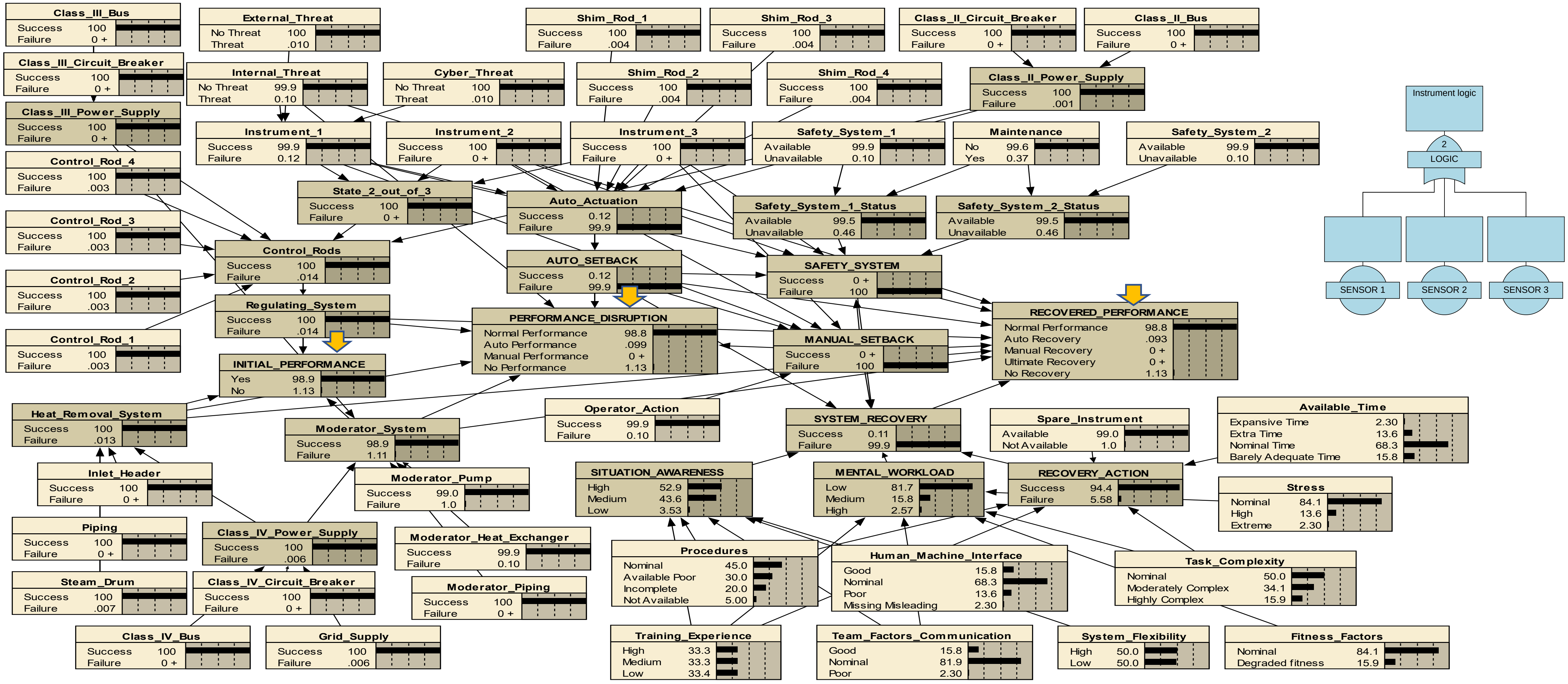


- Possible threat
  - Internal, External or Cyber threat on 2–out-of-3 instrumentation circuit

- Parameter for resilience of system under threat is the steady state availability of reactor system comprising the regulating system, heat removal system, moderator system and associated power supplies

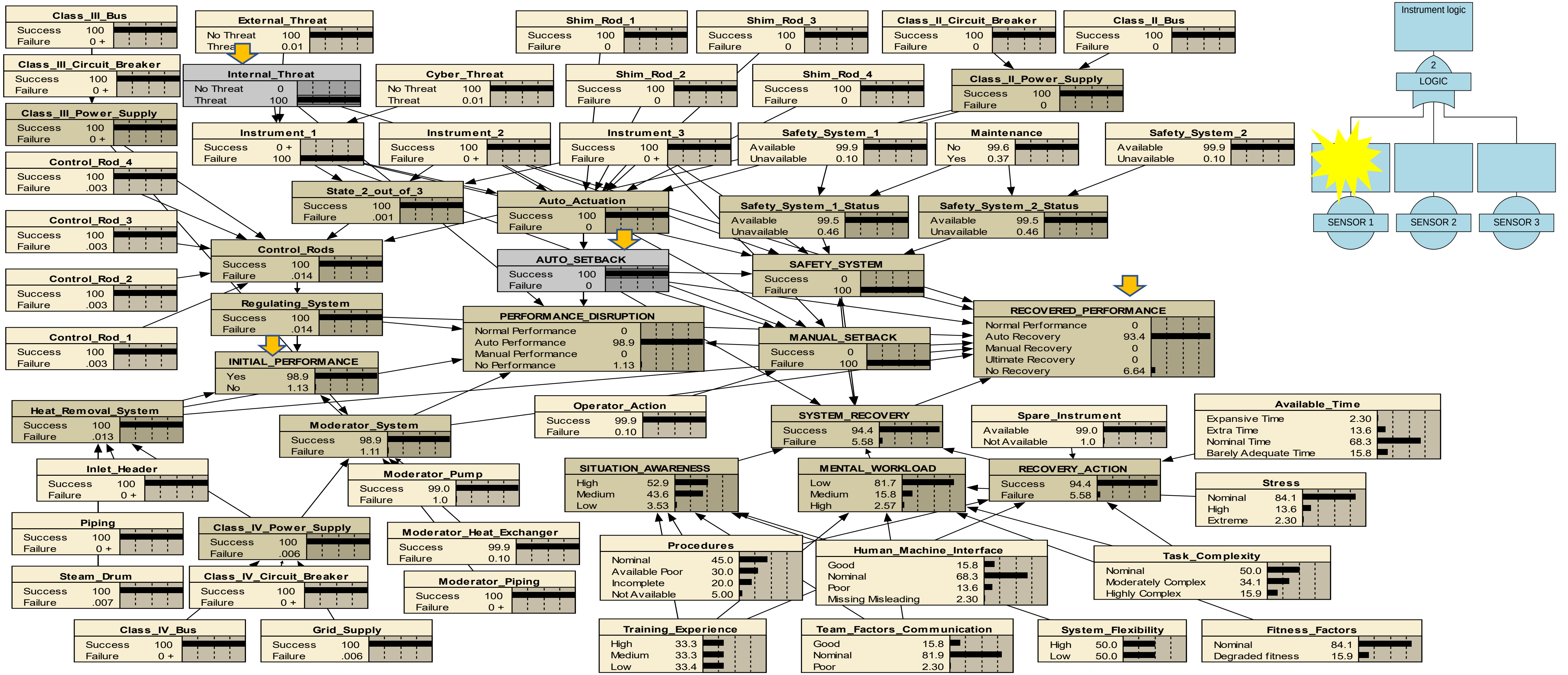
Bayesian model under no threat scenario

- Performance at various stages when there is no threat



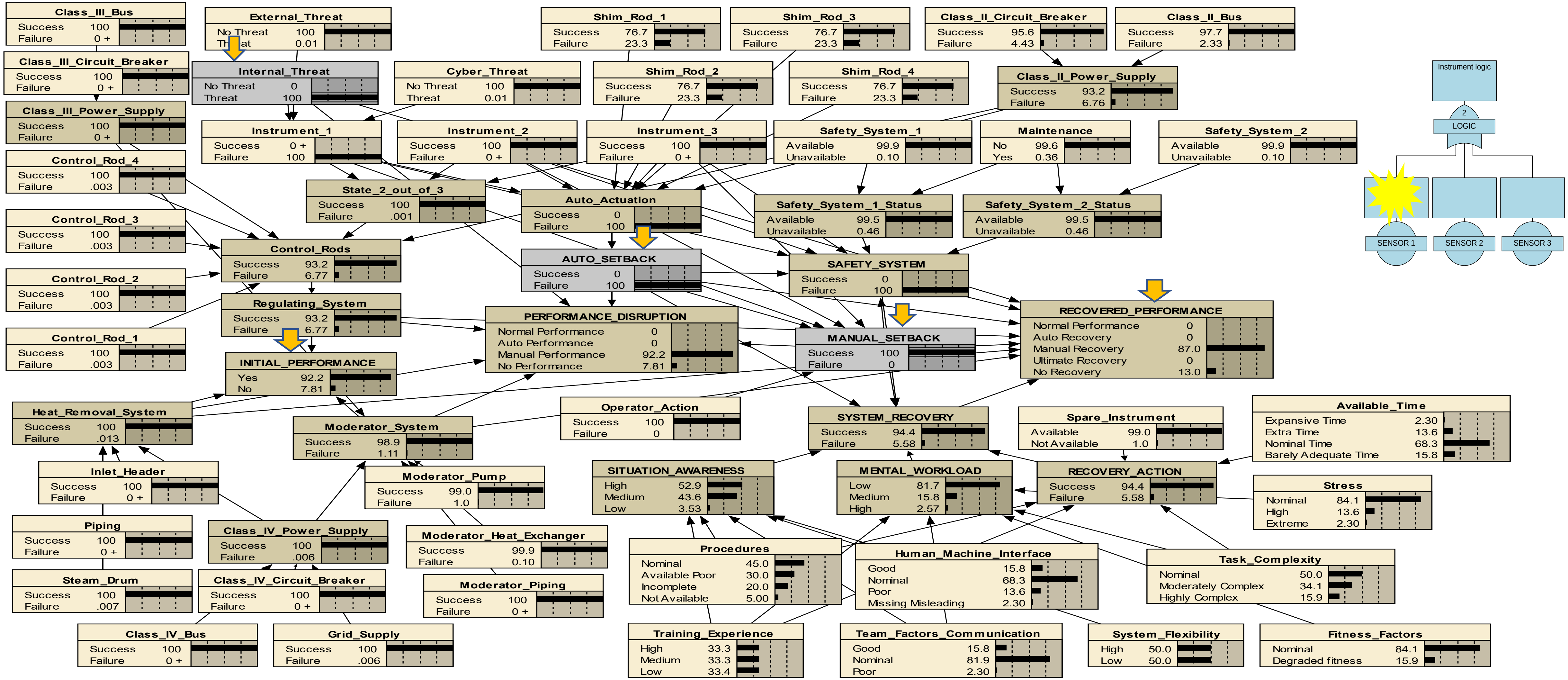
Bayesian model under threat scenario

- Performance at various stages when there is an internal threat on one of the sensors
- Auto setback is working



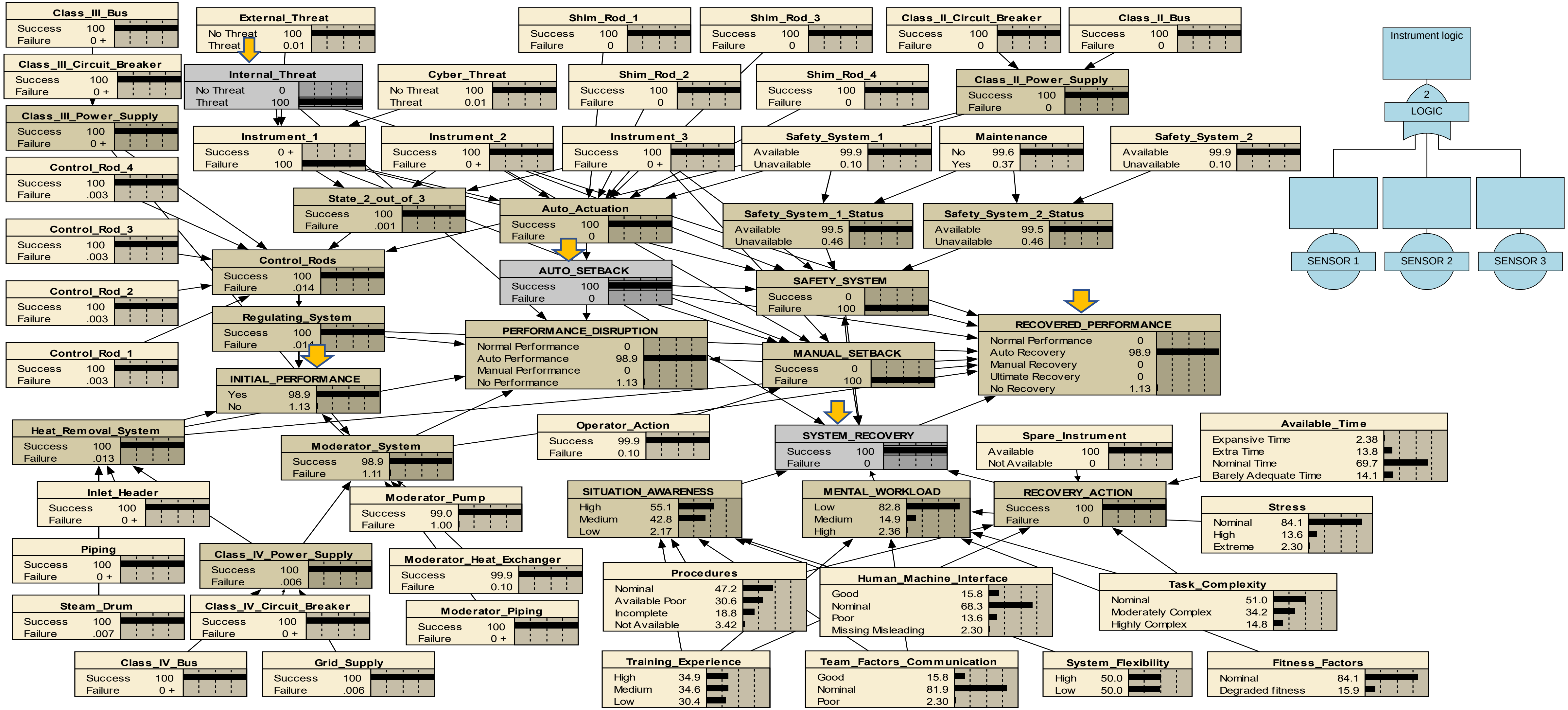
Bayesian model under internal threat

- Performance when there is an internal threat with failure of auto setback
- The performance of the system degrades as the redundancy is lost but all other safety functions are available

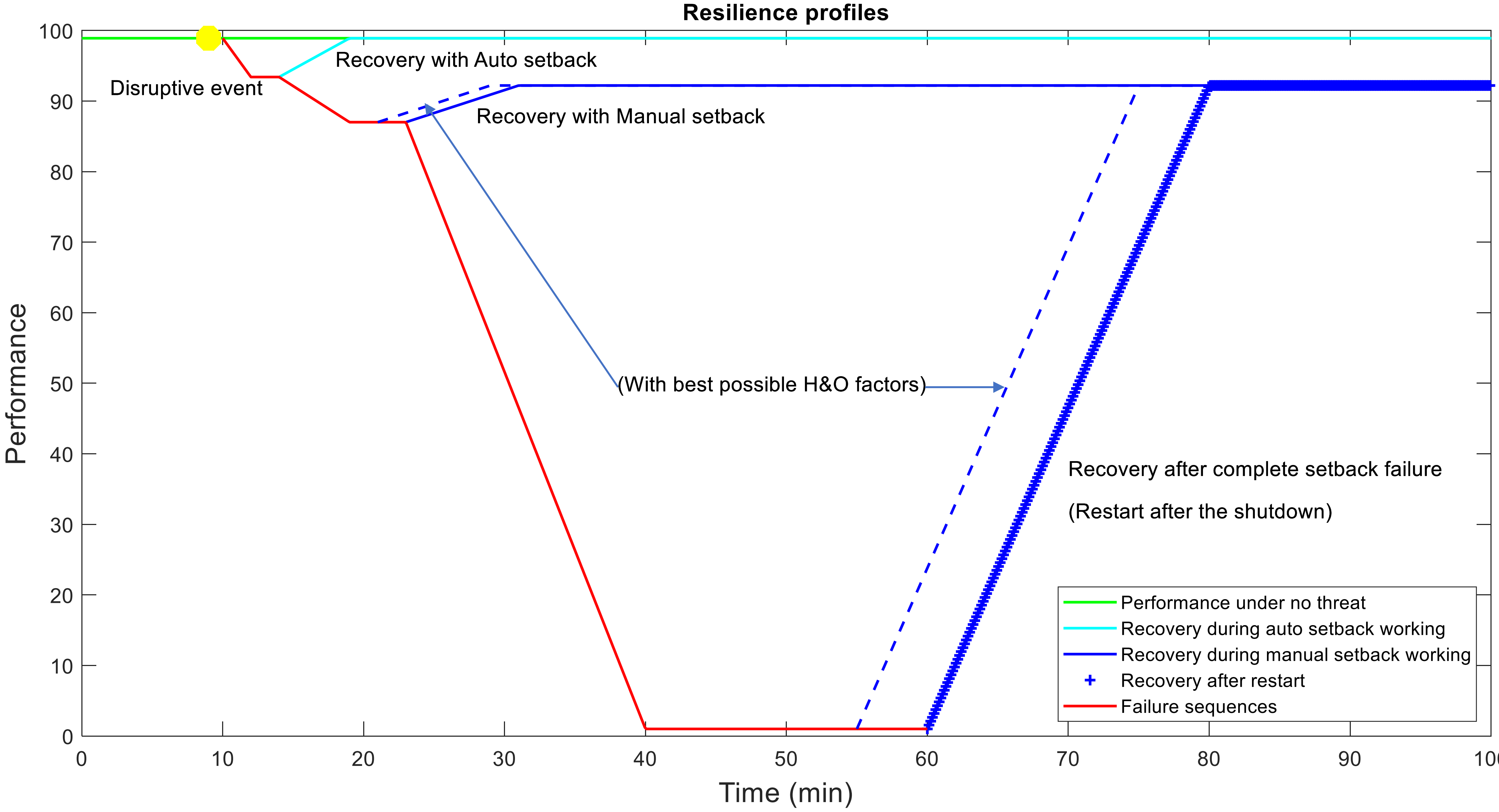


Bayesian model under internal threat

- Performance when recovery implemented



Performance and restoration of reactor system under various threat sequences



Conclusions

- A general framework for resilience assessment of critical infrastructure is developed and applied to a safety related system of an NPP, and resilience profiles have been generated using dynamic Bayesian network.

- This approach integrates the human and organizational factors together with system interactions, and provides quantitative resilience metric over the threat scenarios.

- The approach is flexible for simulating various types of threats, and for generating the possible resilience sequences existing within the system with optimal human and organizational factors.

Thank you for your kind attention