Report of research project on the key technologies for intelligent risk-informed decision support system for nuclear safety and emergency response management with highlighting upgrade of GO-FLOW for success path planning and exact quantification support

Presenter: Jun Yang

March 27, 2024

South China University of Technology

Outline

- Project Background
- Contents of Cooperation
  - Risk layering for safety supervisory and management
  - CAD-based GO-FLOW automatic modeling and analysis platform
  - Task and success path planning for emergency response management
- Future works

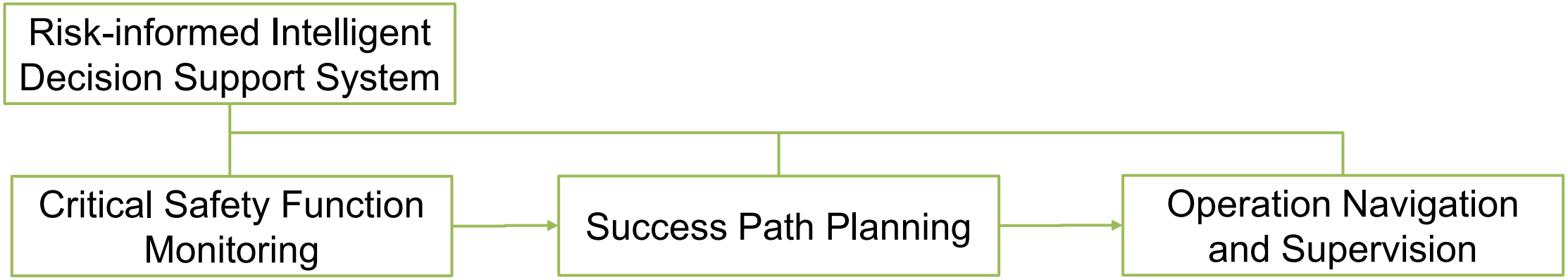
PROJECT BACKGROUND

Project Title: Research on the key technologies for intelligent risk-informed decision support system for nuclear safety and emergency response management

Project Duration (2 years): 2022/1/1~2023/12/30

Organizations	Representatives	Contents of Cooperation
Non-profit Organization Symbio Community Forum (Japan)	Prof. Hidekazu Yoshikawa	1. Risk layering for safety supervisory and management. 2. Development of a CAD-based GO-FLOW automatic modeling and analysis platform. 3. Task and success path planning for emergency response management in the early stage of accident mitigation and recovery. 4. Towards system flow monitoring for Living PSA applications and risk intelligence.
Utsunomiya University (Japan)	Prof. Takeshi Matsuoka	
Shenzhen University (China)	Prof. Ming Yang	
South China University of Technology (China)	Jun Yang	

Part I: Risk layering for safety supervisory and management



Intelligent Risk-informed Decision Support System

The intelligent risk-informed decision support system aims to implement, integrate and maintain success paths to hazard mitigation with planning efforts for risk-layering safety supervisory and management. The intelligent risk-informed decision support system consists of three parts: i) *critical safety function monitoring*; ii) *success path planning*; iii) *operation navigation and supervision*.

Critical safety function monitoring: provide an overview of the safety status of the plant.

Success path planning: provide countermeasures to unexpected events under extreme conditions.

Operation navigation and supervision: provide procedural guidance to operators for efficient task execution and in-process human interaction supervisory.

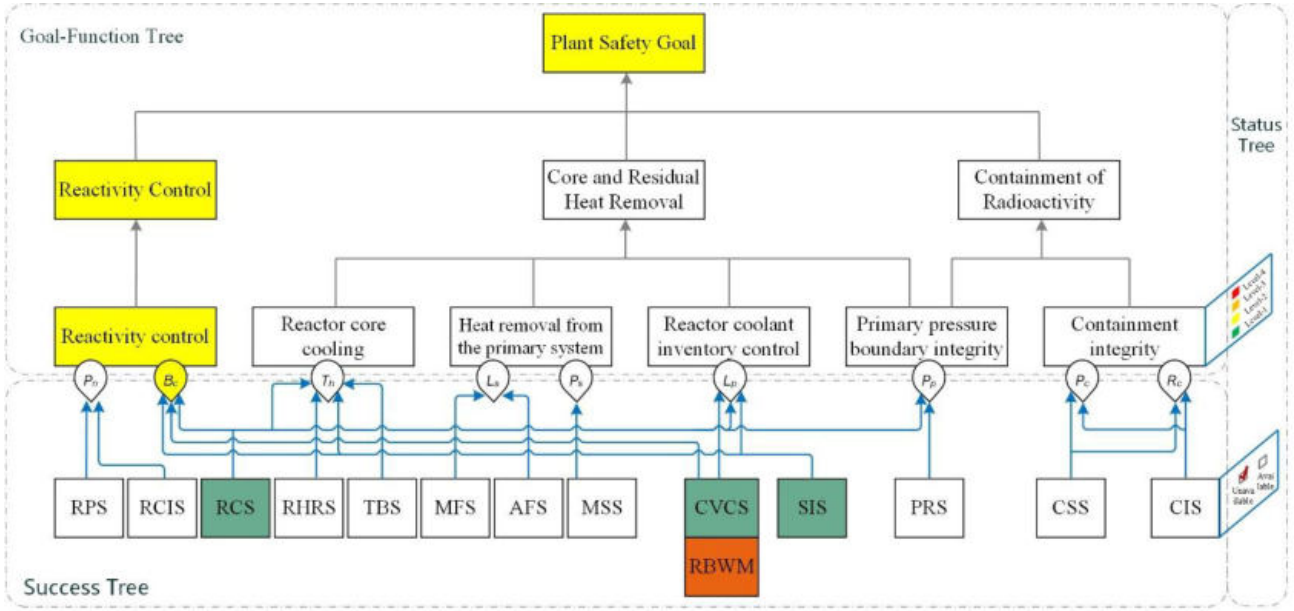
Part I: Risk layering for safety supervisory and management

Critical Safety Function Monitoring

The Critical Safety Function (CSF) monitoring subsystem is designed to be consistent with the Safety Parameter Display System (SPDS) and the Intelligent Alarm System design in nuclear power plants.

The CSF monitoring system is developed using a deep knowledge approach, where complex engineering system domain knowledge is represented by **the coupled goal-function tree, success tree, and state tree models**.

- *Goal-function tree*: *decomposition of Goals-Functions.*
- *Success tree*: *means (process and success paths) to realize functions.*
- *State tree*: *status of CSF and systems components.*



Coupling tree model for knowledge representation

The nuclear safety goal can be achieved and safeguarded by the following 6 critical safety functions:

1. *Reactivity control*
2. *Reactor core cooling*
3. *Heat removal from the primary system*
4. *Reactor coolant inventory control*
5. *Primary pressure boundary integrity*
6. *Containment integrity*

Part I: Risk layering for safety supervisory and management

Critical Safety Function Monitoring

The status of the critical safety functions is defined in accordance with the severity of the process disturbance. The severity of the process disturbance is again manifested by the alarm system design.

Is it possible to correlate the status of the critical safety functions with the alarm priorities?

In general, alarms can be divided into multiple priorities based on its severity and time to respond.

State	Description	Alarm Priority /Severity Level
Negligible	The critical safety function is operational.	1
Moderate	The critical safety function is partially degraded.	2
Critical	The integrity of a critical safety function is severely damaged.	3
Catastrophic	The integrity of a critical safety function is completely lost.	4

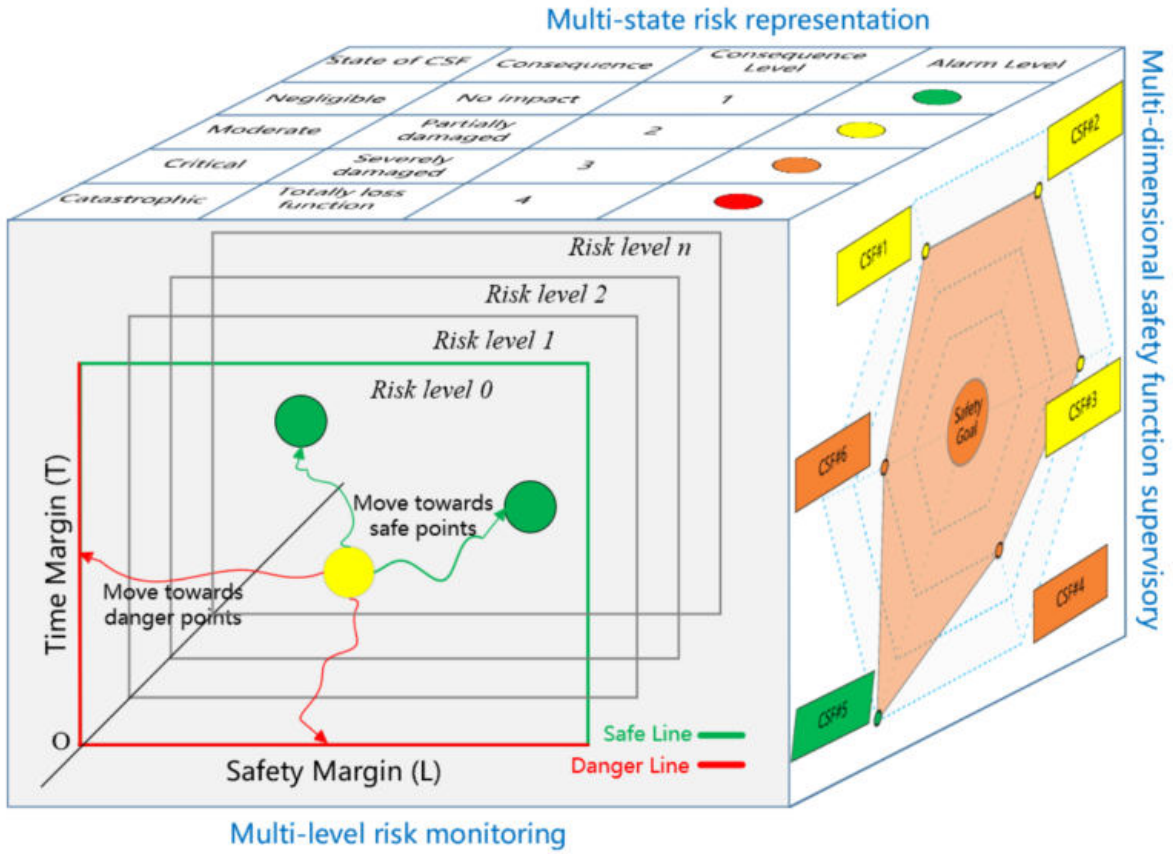
Given the multi-state definition of the critical safety functions, the overall plant safety status can be assessed based on the comprehensive integration of the state of each critical safety function. However, *how to evaluate the overall plant safety status especially from a risk perspective?*

Part I: Risk layering for safety supervisory and management

Critical Safety Function Monitoring

Try it! **Extended all the way up: to integrate the CSF monitoring with multi-valued state definition into Defense-in-Depth (DiD) risk monitor.**

Risk level	Stop	Cool	Contain	Possibility of severe accident
0	1	1	1	No risk Safely shutdown, cooled and no release
1	1	1	0	No severe accident phenomena but some problem in containment
2	1	0	1	Loss of not so serious cooling function Safely shutdown, but cooling failed but no release
3	1	0	0	Serious severe accident possible Safely shutdown, but both cooling and contain function failed
3	0	1	1	Severe accident may be suppressed by ESF function Shutdown failed but cooling and no release
3	0	1	0	Some contain function failed Shutdown failed , cooled but released
4	0	0	1	Serious though severe accident phenomena occurr because containment function succeeded Shutdown failed , cooling failed but no release
5	0	0	0	Worst severe accident because all safety functions failed



Multi-criteria risk classification to build a comprehensive safety risk monitoring and management framework.

Part II: CAD-based GO-FLOW automatic modeling and analysis platform

Innovation of GO-FLOW

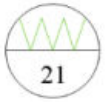
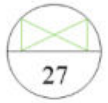
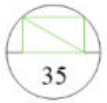
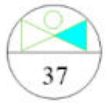
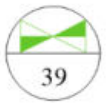
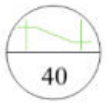
☑ **An automated GO-FLOW modeling tool** is developed to support reliability-based system engineering design and dynamic system reliability analysis.

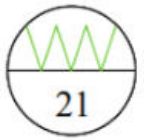
☑ **An exact GO-FLOW solver** is developed to expand the capabilities of powerful computation with the exact solution in both minimum path sets (MPSs) and minimum cut sets (MCSs) representation.

☒ **A versatile GO-FLOW computational platform**: to be developed to augment with availability analysis of repairable PMS system, common cause failure/importance analysis/sensitivity analysis, visual presentation of results for further expansion and optimization.

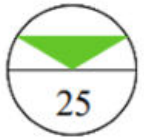
Part II: CAD-based GO-FLOW automatic modeling and analysis platform

GO-FLOW Methodology: all possible system operational state and time-dependent dynamic reliability characteristics can be molded by a series of **GO-FLOW operators and signals** in a logical structure.

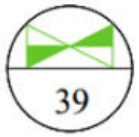
 Two-State Component	 OR Gate	 NOT Gate	 Difference Operator
 Signal Generator	 Normally Closed Component	 Normally Open Component	 Delay Operator
 AND Gate	 Operating Failure of Component	 Standby Failure of Component	 Maintenance of Component
 Opening and Closing Action	 Phased Mission Operator	 Main Input Signal  Sub-input Signal	 Final Signal



Good/failure state of a component: tube



Source signal: water tank

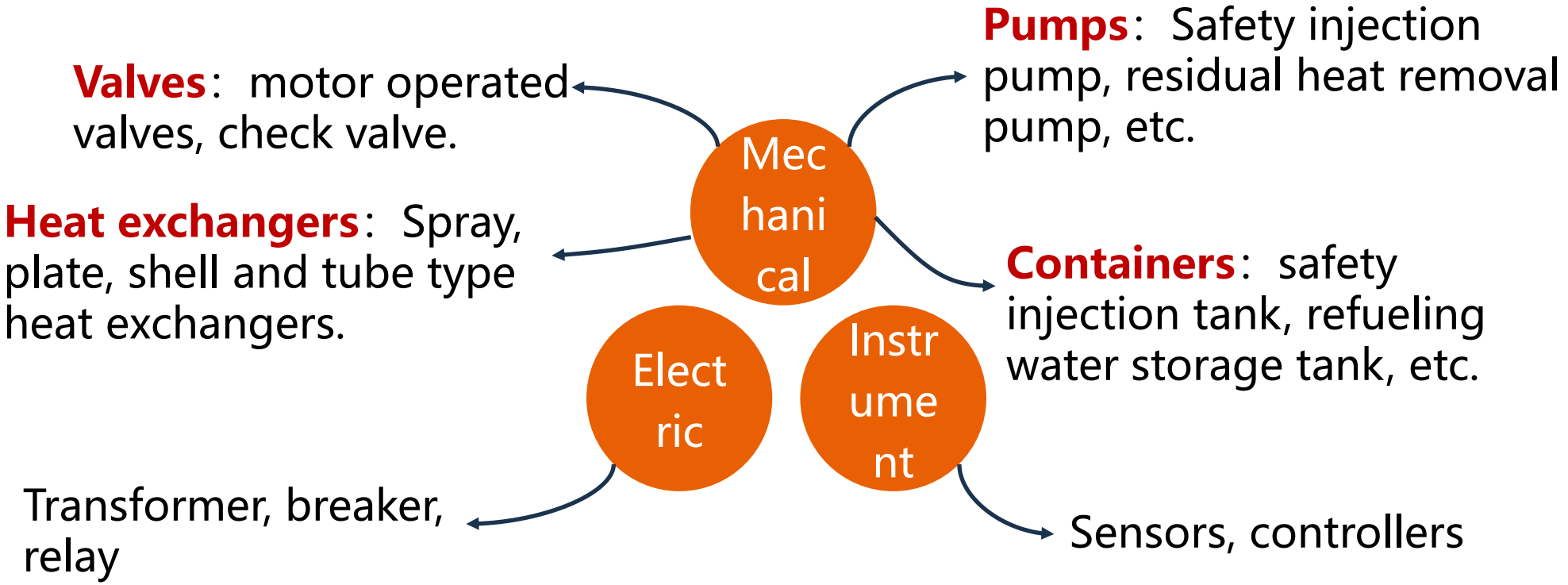


Action component: pump

Part II: CAD-based GO-FLOW automatic modeling and analysis platform

Classification and Categorization of Components + Failure Modes and Effects Analysis

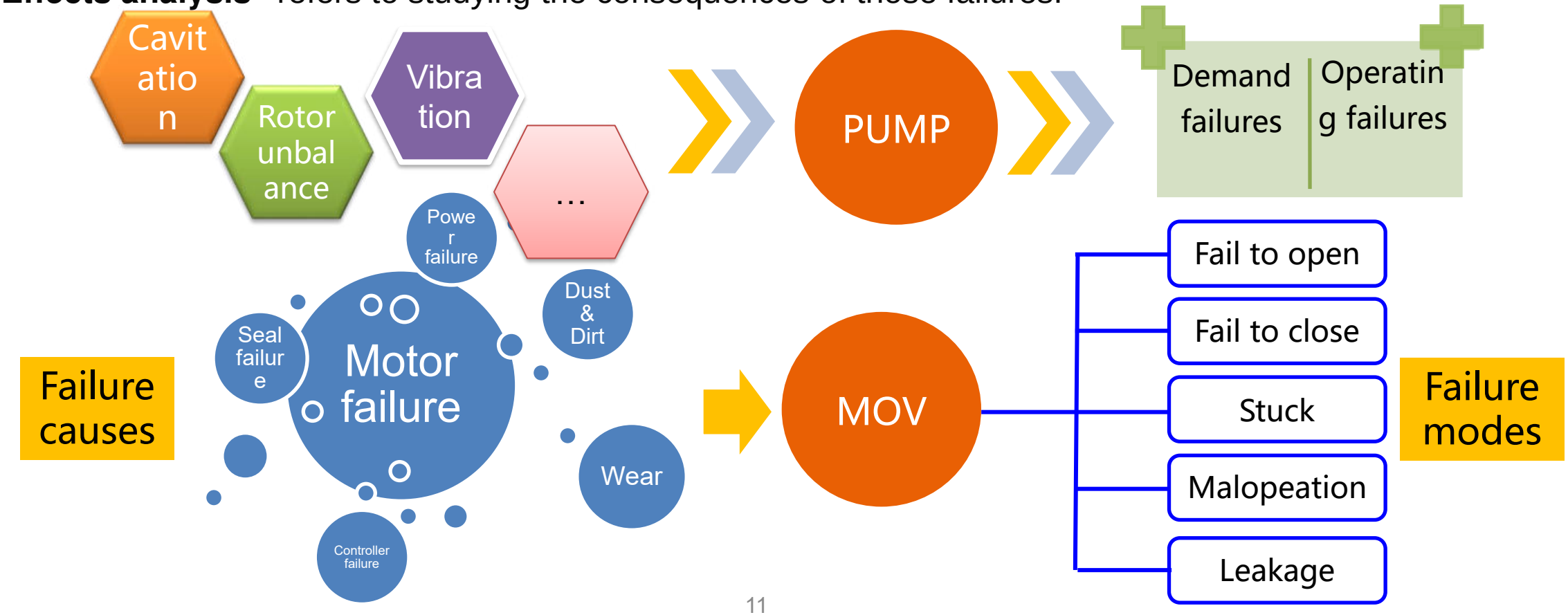
Establish the mapping relationships between the various failure modes of different types of components and GO-FLOW modeling elements to facilitate the componentized modeling.



Part II: CAD-based GO-FLOW automatic modeling and analysis platform

Failure Modes and Effects Analysis: a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.

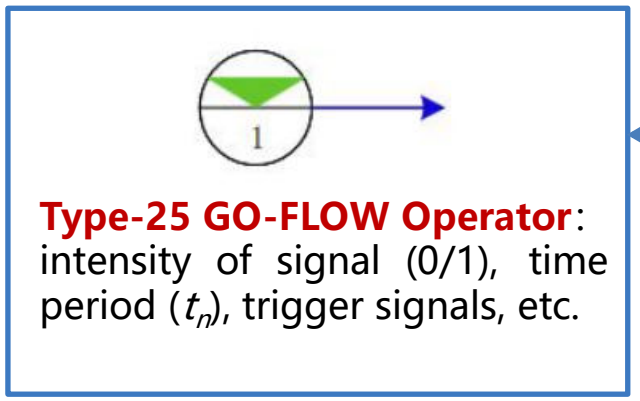
- **"Failure modes"** means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual.
- **"Effects analysis"** refers to studying the consequences of those failures.



Part II: CAD-based GO-FLOW automatic modeling and analysis platform

Componentized GO-FLOW modeling structure: Basic reliability characteristics+aging effects +maintenance signals+… +phased missions +time delay of

- Two-state components
- Normally open components
- Normally close components
- Switching components



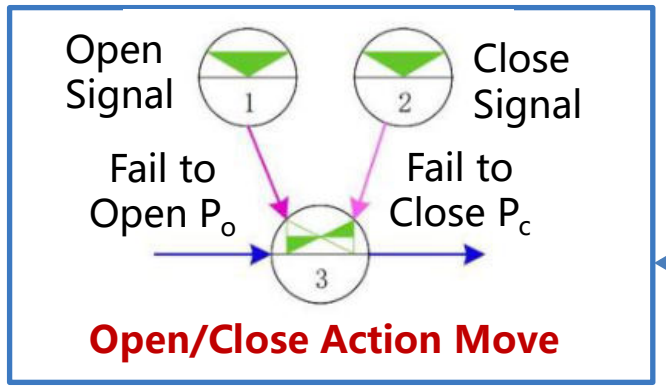
Type-25 GO-FLOW Operator: intensity of signal (0/1), time period (t_n), trigger signals, etc.

Source signal/control signal

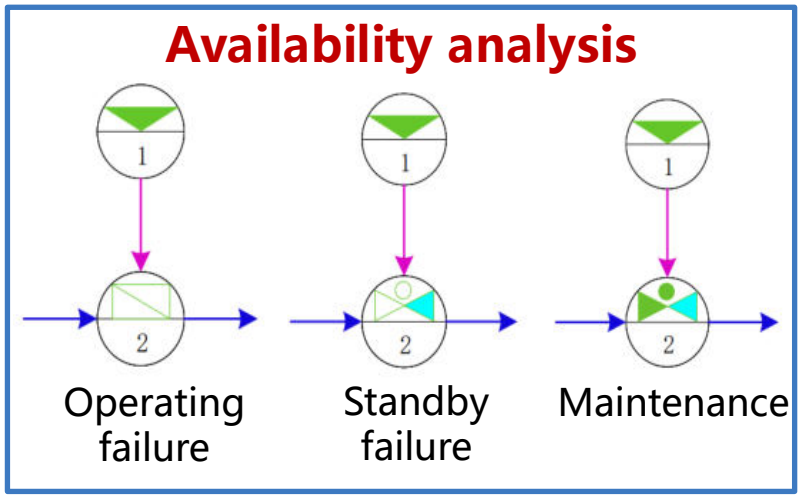
Operating failures

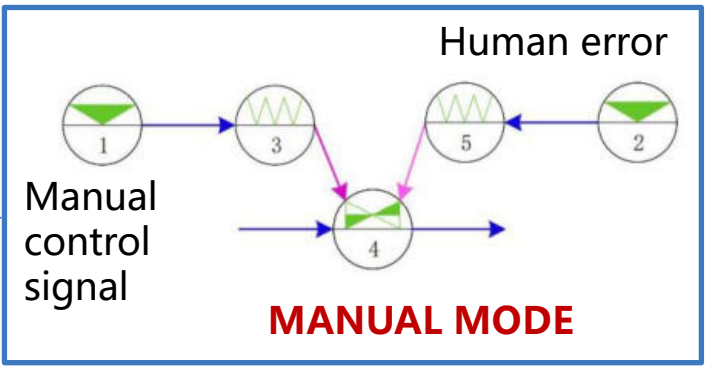
Control Modes

Demand failures



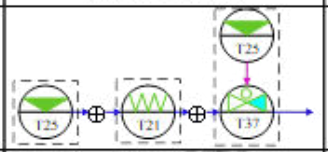
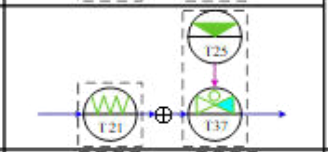
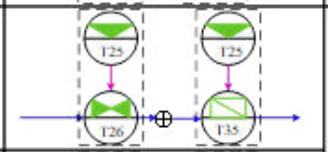
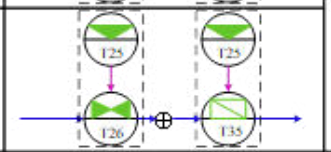
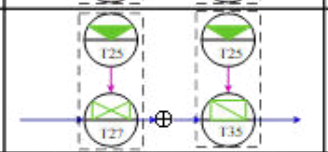
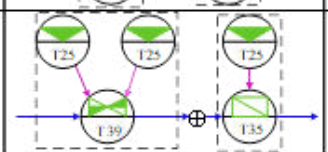
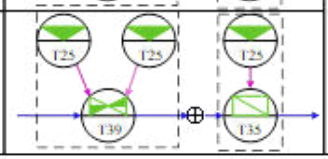
Open/Close Action Move





Part II: CAD-based GO-FLOW automatic modeling and analysis platform

A collection of componentized GO-FLOW model representation for the most commonly used equipment

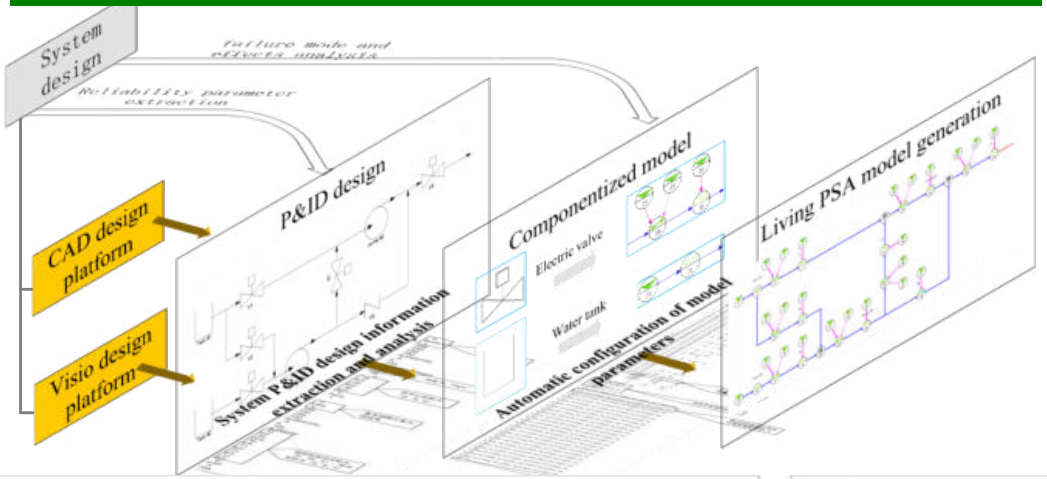
Categories	Sub-categories	Types of components	Function/failure modes	Componentized GO-FLOW model	Reliability parameter	Output intensity
Non-action component	Source component	Container	Signal source ⊕ Good/Damage state ⊕ Leakage failure on performance over time		Output signal: $S(t)$ Probability of failure on demand: P_g Failure rate: λ Repair rate: μ	$R(t)=S(t)\cdot R_1(t)\cdot R_2(t)$ $R_1(t)=P_g$ $R_2(t)=\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)\times\sum_i\sum_{t_n}P(t_n)}$
	Non-source component	Heat Exchanger	Good/Damage state ⊕ Failure on performance over time (Blockage, Leakage)		Probability of failure on demand: P_g Failure rate: λ Repair rate: μ	$R(t)=S(t)\cdot R_1(t)\cdot R_2(t)$ $R_1(t)=P_g$ $R_2(t)=\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)\times\sum_i\sum_{t_n}P(t_n)}$
		Check Valve	Good/Damage state ⊕ Failure on performance over time (Leakage)			
Action component	Normally closed component	Relief Valve / Safety Valve	Fail open ⊕ Failure in operations (Leakage)		Probability of pre-action: P_p Probability of failure on demand: P_g Failure rate: λ Repair rate: μ	$R(t)=S(t)\cdot R_1(t)\cdot R_2(t)$ $\begin{cases} R_1(t)=S(t)\cdot O(t) \\ O(t_1)=P_p \\ O(t_n)=O(t_{n-1})+\left[1-O(t_{n-1})\right]\cdot P(t_n)\cdot P_g \end{cases}$ $R_2(t)=S(t)\times\left\{\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)\times\sum_i\sum_{t_n}\left[P(t_n)\times\min\left(1.0,\frac{S(t_n)}{S(t)}\right)\right]}\right\}$
		Relay	Fail open ⊕ Failure in operations			
	Normally open component	Fuse and circuit breaker	Fail open ⊕ Failure in operations		Probability of pre-action: P_p Probability of failure on demand: P_g Failure rate: λ Repair rate: μ	$R(t)=S(t)\cdot R_1(t)\cdot R_2(t)$ $\begin{cases} R_1(t)=S(t)\cdot O(t) \\ O(t_1)=P_p \\ O(t_n)=O(t_{n-1})\cdot\left[1-P(t_n)\cdot P_g\right] \end{cases}$
	Switching component	Motor Operated Valve / Manually Operated Valve / Regulating Control Valve	Fail on demand (Fail open / Fail closed) ⊕ Failure in operations		Probability of pre-action: P_p Shutdown failure: P_c Startup failure: P_o Failure rate: λ Repair rate: μ	$R(t)=S(t)\cdot R_1(t)\cdot R_2(t)$ $\begin{cases} R_1(t)=S(t)\cdot O(t) \\ O(t_1)=P_p \\ O(t_n)=O(t_{n-1})+\left[1-O(t_{n-1})\right]\cdot P_1(t_n)\cdot P_o \\ O(t_n)=O(t_{n-1})\cdot\left[1-P_2(t_n)\cdot P_c\right] \end{cases}$ $R_2(t)=S(t)\times\left\{\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)\times\sum_i\sum_{t_n}\left[P(t_n)\times\min\left(1.0,\frac{S(t_n)}{S(t)}\right)\right]}\right\}$
		Pump	Fail on demand (Fail open / Fail closed) ⊕ Failure in operations			

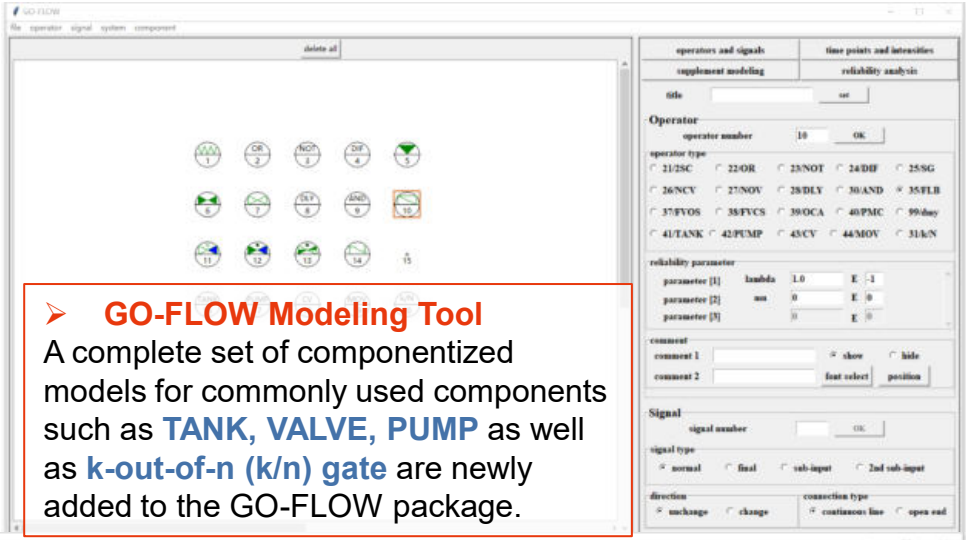
Part II: CAD-based GO-FLOW automatic modeling and analysis platform

Objectives

: generate system reliability model directly from system **Piping and Instrumentation Diagram (P&ID)** drawings so as to improve the consistency, accuracy, and convenience of the reliability and risk modeling process[1-2].

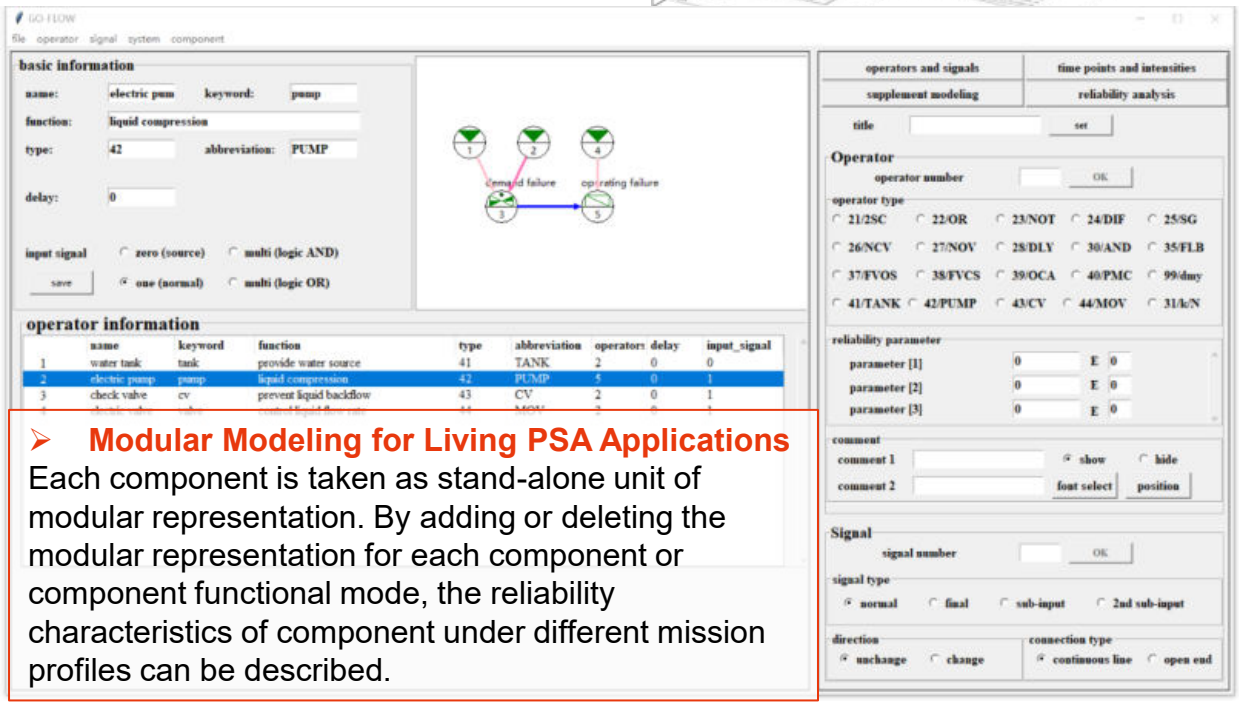
Framework for automated GO-FLOW model generation





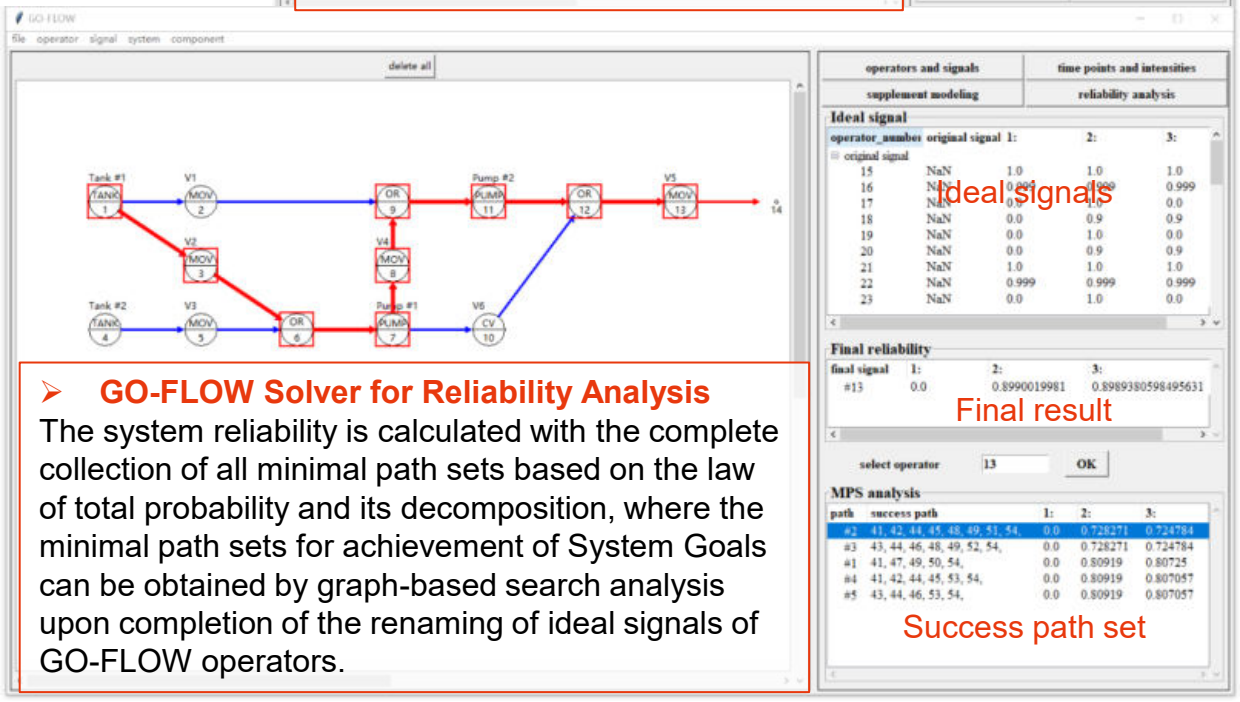
➢ **GO-FLOW Modeling Tool**

A complete set of componentized models for commonly used components such as **TANK, VALVE, PUMP** as well as **k-out-of-n (k/n) gate** are newly added to the GO-FLOW package.



➢ **Modular Modeling for Living PSA Applications**

Each component is taken as stand-alone unit of modular representation. By adding or deleting the modular representation for each component or component functional mode, the reliability characteristics of component under different mission profiles can be described.



➢ **GO-FLOW Solver for Reliability Analysis**

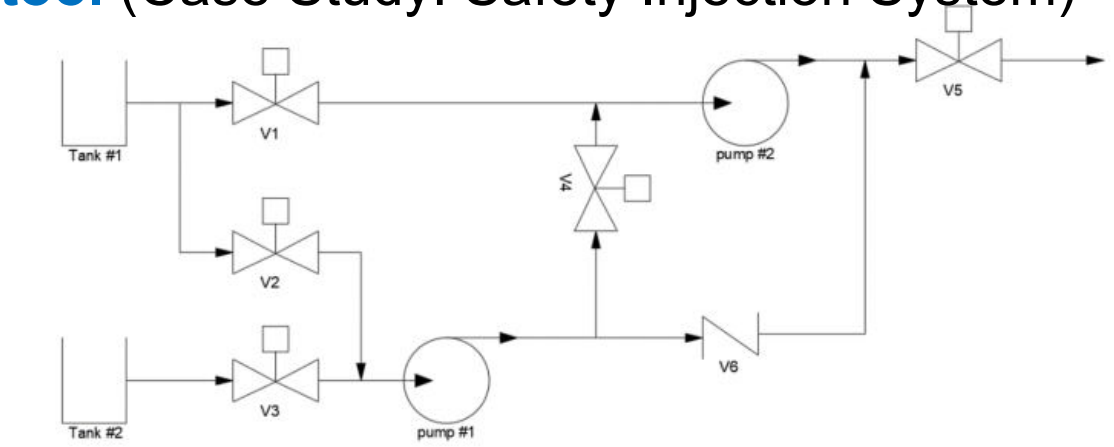
The system reliability is calculated with the complete collection of all minimal path sets based on the law of total probability and its decomposition, where the minimal path sets for achievement of System Goals can be obtained by graph-based search analysis upon completion of the renaming of ideal signals of GO-FLOW operators.

Part II: CAD-based GO-FLOW antomatic modeling and analysis platform

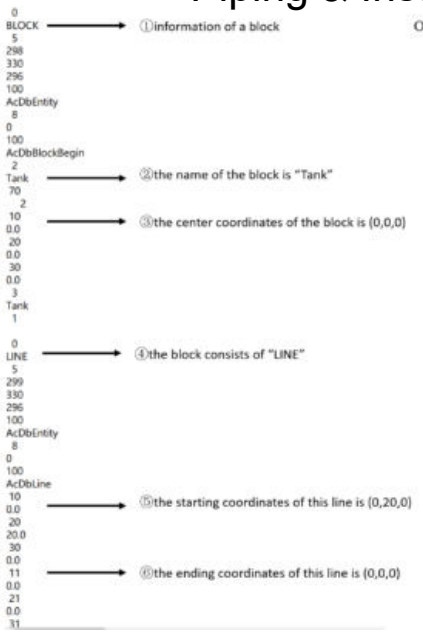
☑ II-1: An automated GO-FLOW modeling tool (Case Study: Safety Injection System)

Categories	Sub-categories	Types of components	Failure modes	Reliability parameters	Componentized GO-FLOW model
Non-action Component	Source component	Container	Leakage	Probability of Failure on demand P_g	
	Non-source component	Heat exchanger	Blockage, leakage	Failure rate λ Repair rate μ	
		Check valve	Blockage, leakage	Failure rate λ Repair rate μ	
Action Component	Normally closed component	Relief Valve/ Safety Valve	Leakage, fail open	Probability of action of time P_p Probability of Failure on demand P_g	
		Relay	Overload, wear out	Probability of action of time P_p Probability of Failure on demand P_g	
	Normally open component	Fuse and circuit breaker	Fail closed	Probability of action made ahead of time P_p Probability of Failure on demand P_g	
	Switching component	Motor Operated Valve / Manually Operated Valve/ Regulating Control Valve/	Failure on demand (Fail Open / Fail Closed)	Probability of action ahead of time P_p Shutdown failure P_c Startup failure P_o Failure rate λ Repair rate μ	
		Pump	Failure of demand, operating failure	Probability of action ahead of time P_p Shutdown failure P_c Startup failure P_o Failure rate λ Repair rate μ	

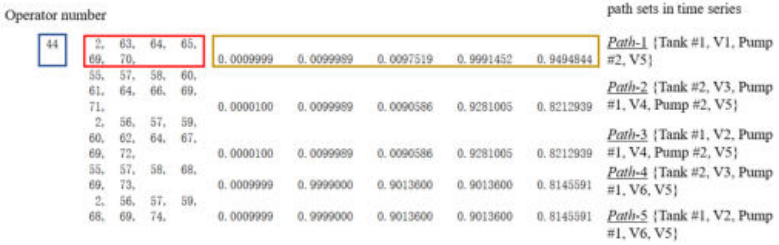
Componentized GO-FLOW model library



Piping & Instrumentation Diagram drawing



Data Parsing



The success path sets are listed as follows: {*Path*-1: Tank #1, V1, Pump #2, V5}, {*Path*-2: Tank #2, V3, Pump #1, V4, Pump #2, V5}, {*Path*-3: Tank #1, V2, Pump #1, V4, Pump #2, V5}, {*Path*-4: Tank #2, V3, Pump #1, V6, V5}, {*Path*-5: Tank #1, V2, Pump #1, V6, V5}.

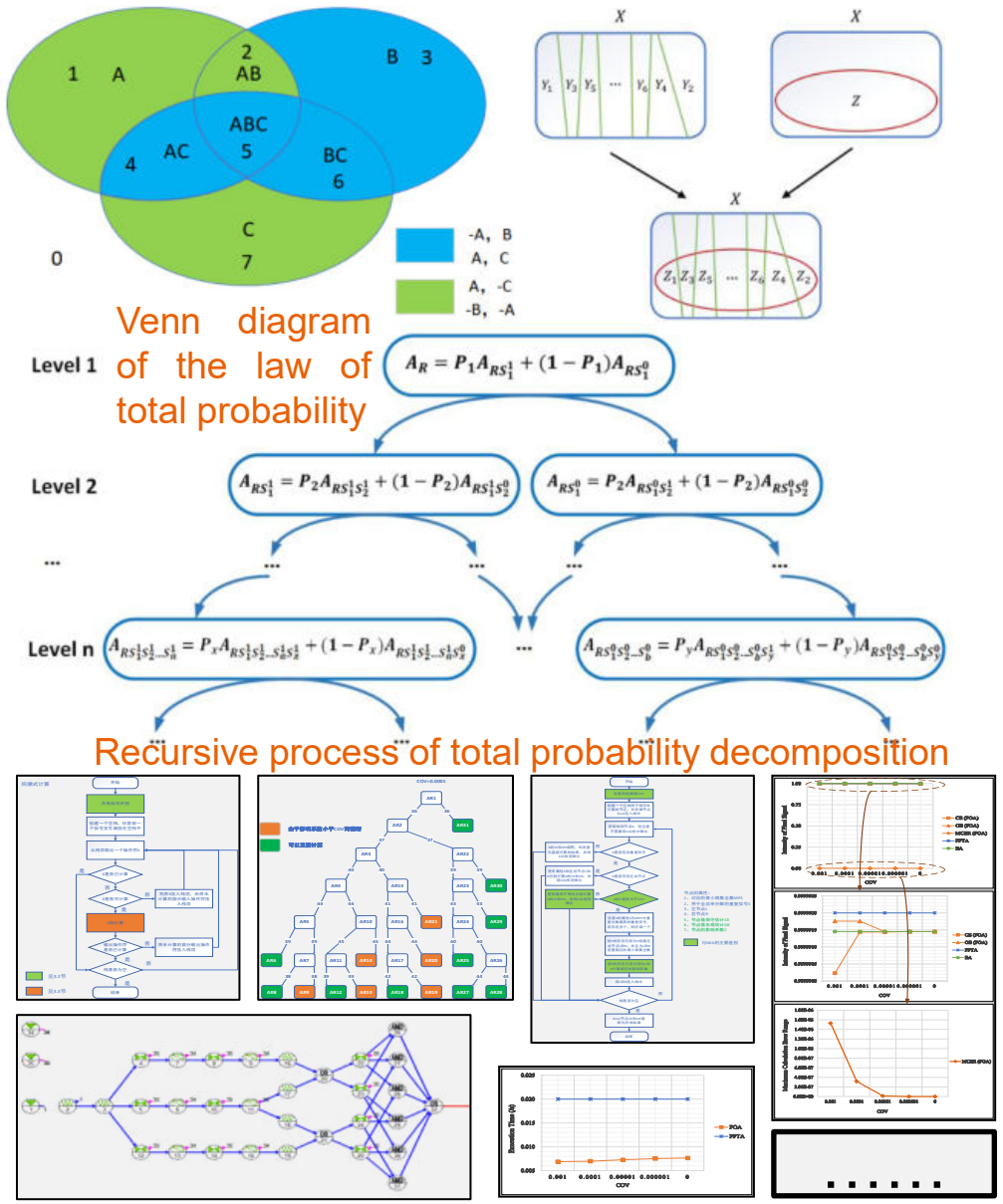
Part II: CAD-based GO-FLOW antomatic modeling and analysis platform

❑ II-2: An exact GO-FLOW Solver[3]

By applying the law of total probability and its recursive decompositions, an exact GO-FLOW solver is developed to effectively capture the *dynamic operational characteristics* of process engineering systems, identify *failure dependencies (shared signals)* in system GO-FLOW model, obtain both the **minimal path sets/minimal cut sets** from both success and failure perspectives, and *offer scalable and flexible solution* for computing power and application extensions. The algorithm tool is able to offer a much more flexible way to achieve the trade-off between computational complexity and accuracy on the use of cut-off criterion.

◆ Features, Advantages & Benefits (FAB)

- ☑ Capturing for system dynamic timing characteristics
- ☑ Degradation modeling with application to aging and maintenance effectiveness evaluations
- ☑ Phased mission reliability analysis with loop structures
- ☑ The guarantee of exact solutions
- ☑ Flexibility in the balance of computational efficiency and accuracy



Part II: CAD-based GO-FLOW antomatic modeling and analysis platform

☑ II-2: An exact GO-FLOW solver[4]

The algorithm is implemented by the following steps:

Step-1: GO-FLOW modeling.

Step-2: Final signal marking.

Step-3: Shared signal identification.

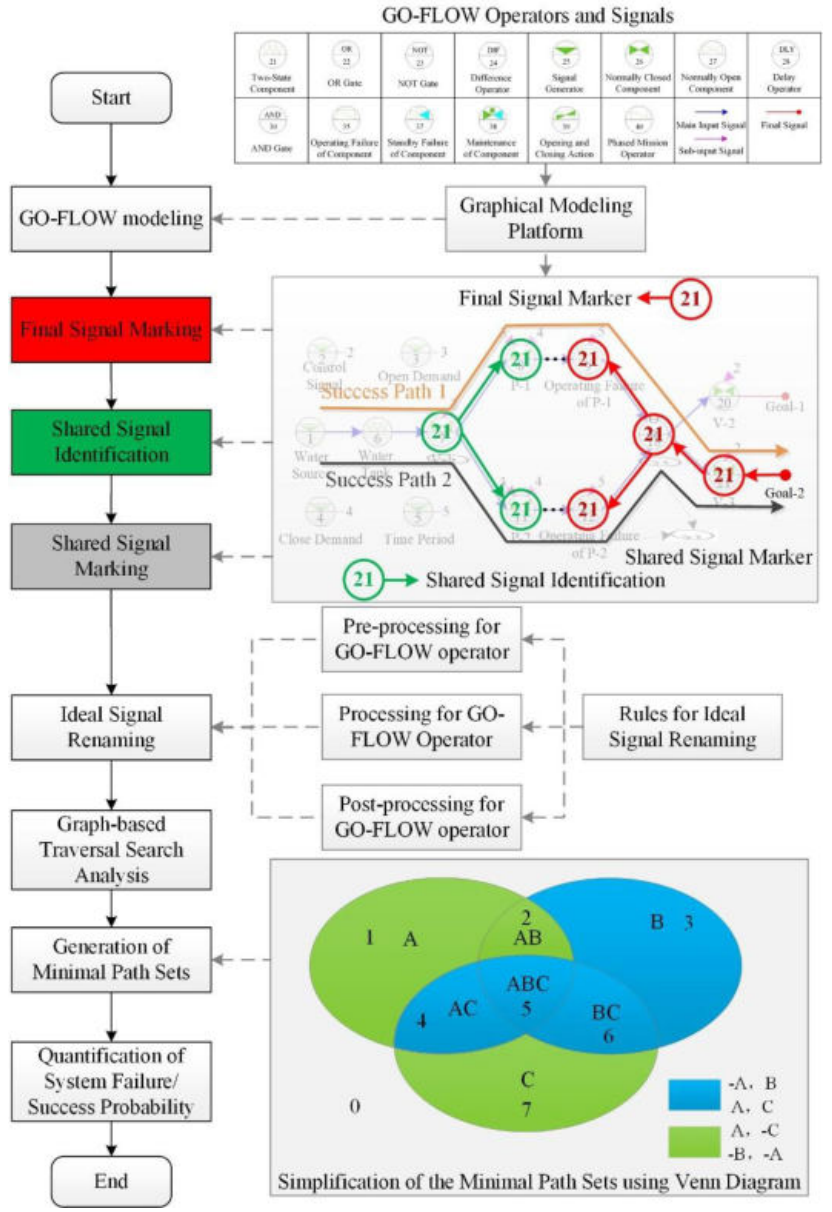
Step-4: Shared signal marking.

Step-5: Ideal signal renaming.

Step-6: Graph-based traversal search analysis.

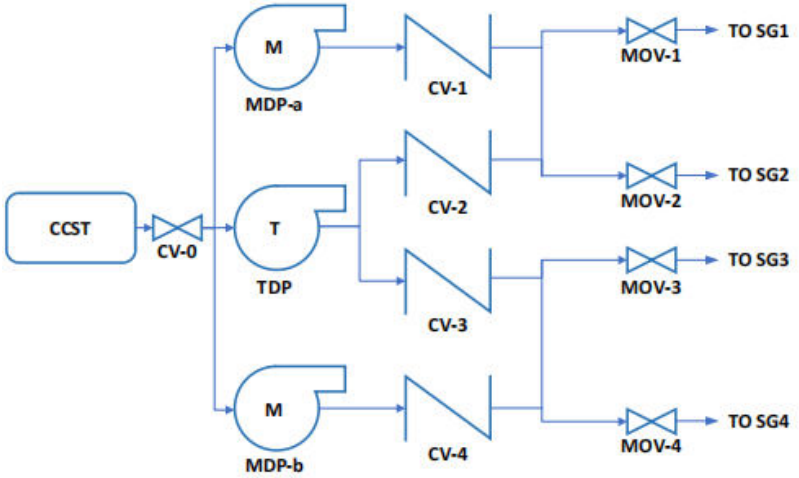
Step-7: Generation of the minimal path sets/minimal cut sets.

Step-8: Quantification of system failure/success probability.

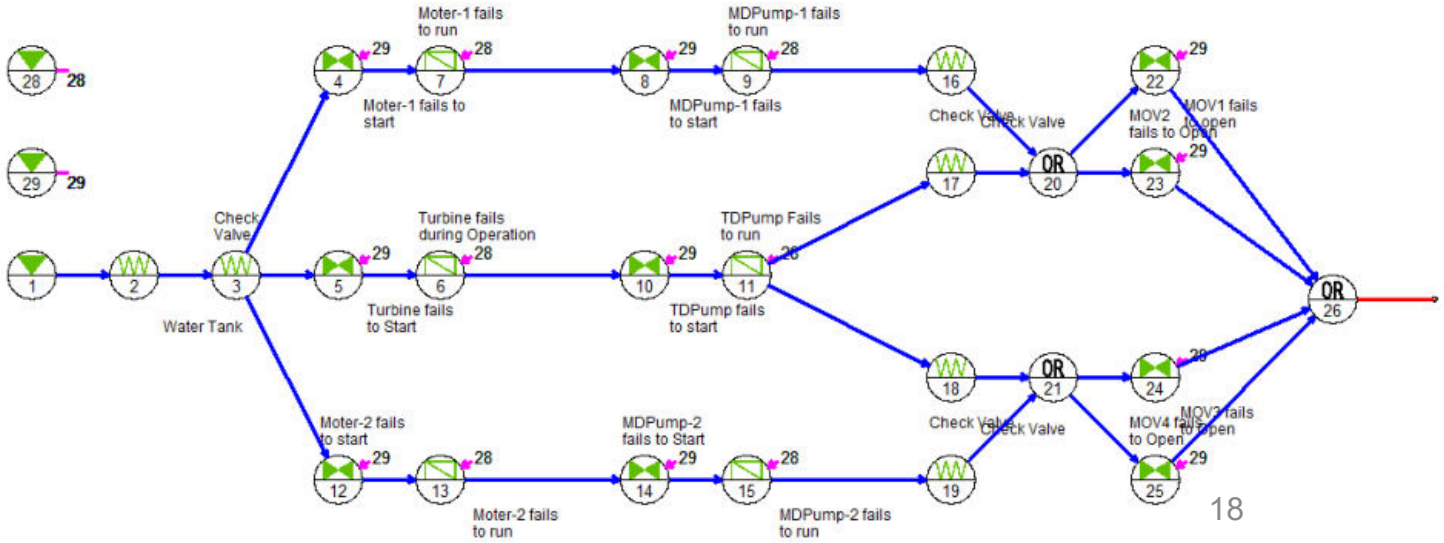


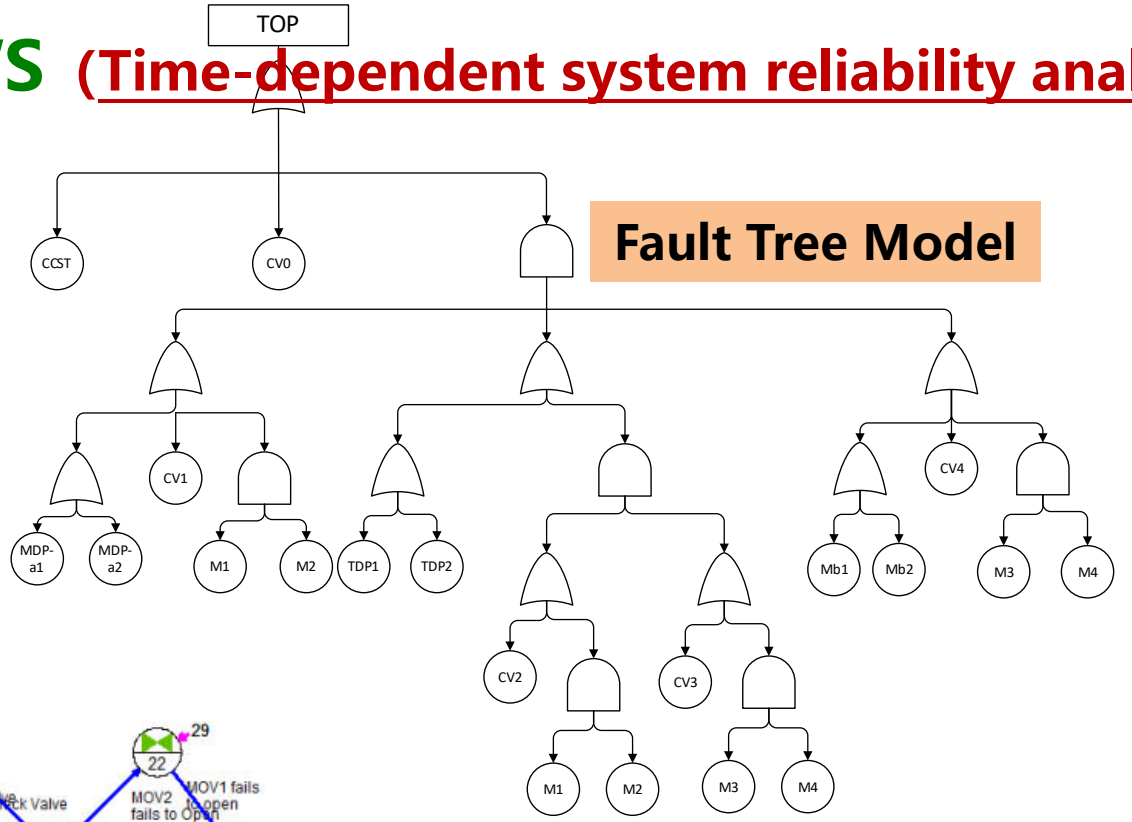
Test of GO-FLOW algorithm for time-dependent system reliability analysis

❑ Case study-I: PWR-AFWS (Time-dependent system reliability analysis)



GO-FLOW Model





Fault Tree Model

Verification Results:

Breakthrough in MCSs solving;

Exact Solution;

Alternative to BDD algorithm.

Method	System Startup Failure	System Operation for 24 hours	Elapsed Time
GO-FLOW	6.088431418e-06	6.23741702898e-06	52ms
BDD	6.088431418e-06	6.23741702898e-06	56ms
MOCUS	6.088433555e-06	6.23741962947e-06	222ms
RS	6.088e-06	6.237e-06	
RWB	6.087e-0	6.328e-06	

Derivation of Minimal Cut Sets by GO-FLOW

MCSs Derivation

The GO-FLOW diagram derivation of MCSs consists of two steps:

- Step #1: Conversion of cut sets from minimal path sets

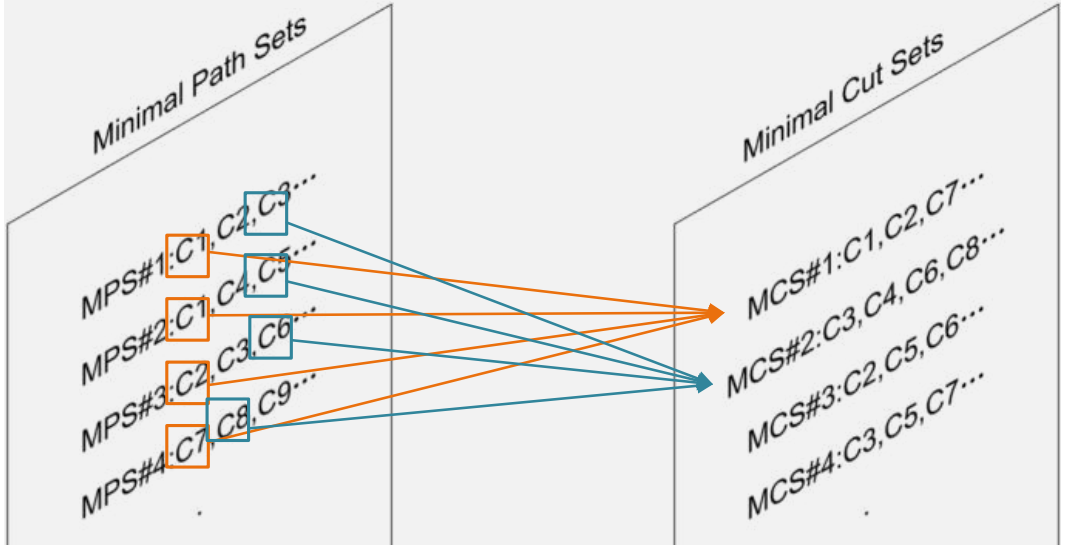
Cut Set: a cut set is a collection of component failure modes that could lead to a system failure.

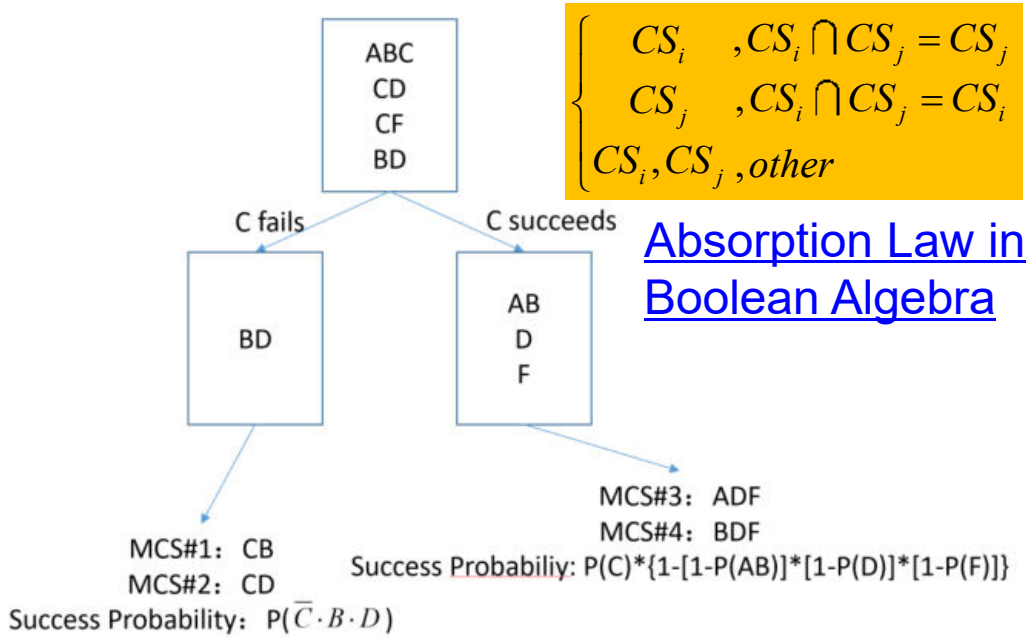
A component is selected to fail from each path, and the set of these failed components is called the cut set. When the same component is identified in multiple success paths, it is reserved for only once.

- Step #2: Optimal solution generation of Minimal Cut Sets

Minimal Cut Set: a cut set that cannot be reduced without losing its status as a cut set for triggering the top event.

A process of reduction using the laws of Boolean algebra is then applied to identify only the truly unique minimal cut sets.





$$\begin{cases} CS_i, CS_i \cap CS_j = CS_j \\ CS_j, CS_i \cap CS_j = CS_i \\ CS_i, CS_j, other \end{cases}$$

Absorption Law in Boolean Algebra

Derivation of Minimal Cut Sets by GO-FLOW

MCSs Derivation (Non-intersecting MCSs in GO-FLOW)

MCSs	BDD	RWB	MOCUS	GO-FLOW
CV0	3.9999920E-06	3.9999920E-06	4.0000000E-06	4.0000000E-06
CCST	2.0000000E-06	1.9999980E-06	2.0000000E-06	2.0000000E-06
Ma Mb TDP	8.5758235E-08	8.4282959E-08	8.5758750E-08	8.5758750E-08
Mb TDP M1 M2	9.5942248E-10	9.4120491E-10	9.6101775E-10	9.6101775E-10
Ma TDP M3 M4	9.5942248E-10	9.4120491E-10	9.6101775E-10	9.6101775E-10
M1 M2 M3 M4	3.4184245E-10	3.3895358E-10	3.4188010E-10	3.4188010E-10
CV1 Mb TDP	2.0755572E-10	2.0449053E-10	2.0790000E-10	2.0790000E-10
Ma CV4 TDP	2.0755572E-10	2.0449053E-10	2.0790000E-10	2.0790000E-10
CV4 TDP M1 M2	2.3220350E-12	2.2835872E-12	2.3297400E-12	2.3297400E-12
CV1 TDP M3 M4	2.3220350E-12	2.2835872E-12	2.3297400E-12	2.3297400E-12
CV1 CV4 TDP	5.0233516E-13	4.9614271E-13	5.0400000E-13	5.0400000E-13
Mb CV3 M1 M2	1.1818922E-13	1.2140134E-13	1.2203400E-12	1.2203400E-12
Ma CV2 M3 M4	1.1818922E-13	1.2141013E-13	1.2203400E-12	1.2203400E-12
CV4 CV3 M1 M2	2.8604656E-16	2.9456990E-16	2.9584000E-15	2.9584000E-15
CV1 CV2 M3 M4	2.8604656E-16	2.9456990E-16	2.9584000E-15	2.9584000E-15
Ma Mb CV2 CV3	4.2187607E-17	4.3488021E-17	4.3560000E-15	4.3560000E-15
CV1 Mb CV2 CV3	1.0210424E-19	1.0551230E-19	1.0560000E-17	1.0560000E-17
Ma CV4 CV2 CV3	1.0210424E-19	1.0551230E-19	1.0560000E-17	1.0560000E-17
CV1 CV4 CV2 CV3	2.4711700E-22	2.5599795E-22	2.5600000E-20	2.5600000E-20

GO-FLOW Solver for Efficient Mission Reliability Analysis

☐ Case Study II: Emergency Core Cooling System

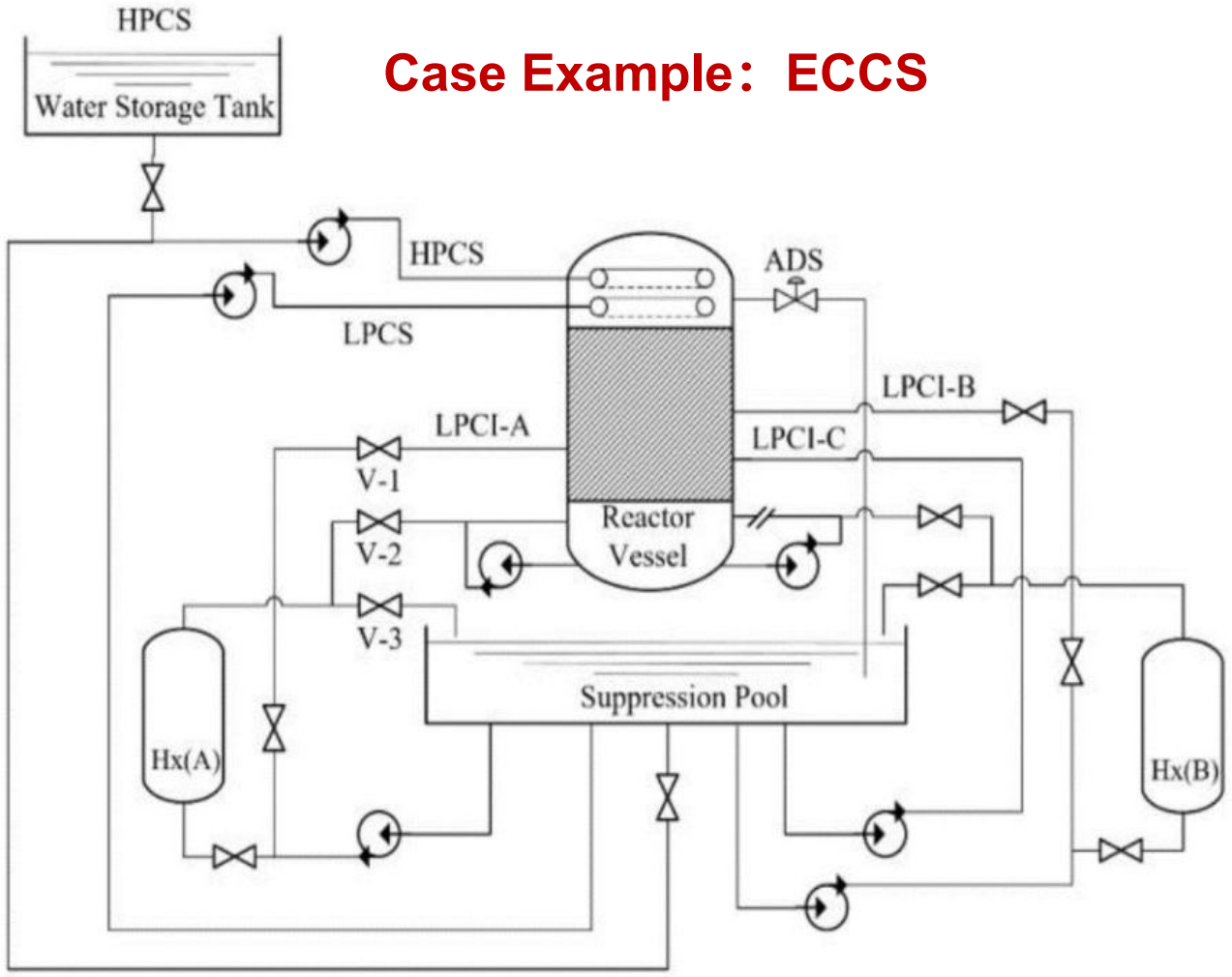
Emergency Core Cooling System (ECCS), as one of the most important safety engineering features in nuclear power plants, is designed to inject the high-concentration borated water into the reactor core following a Loss of Coolant Accident (LOCA) or a Steam Generator Tube Rupture (SGTR).

ECCS consists of a water storage tank (HPCS), two heat exchangers (HX·A, HX·B), automatic depressurization system (ADS), High-Pressure Recirculation Cooling System (HPCS), Low-Pressure Recirculation Cooling System (LPCS), Low-Pressure Core Injection pumps (LPCI-A,B,C), motor operated valves and associated pipelines.

The emergency core cooling system of BWR is a typical phased-mission system.

- **Phase I: initial core cooling (0.5h)**
- **Phase II: suppression pool cooling (36 h)**
- **Phase III: residual heat removal (84 h)**

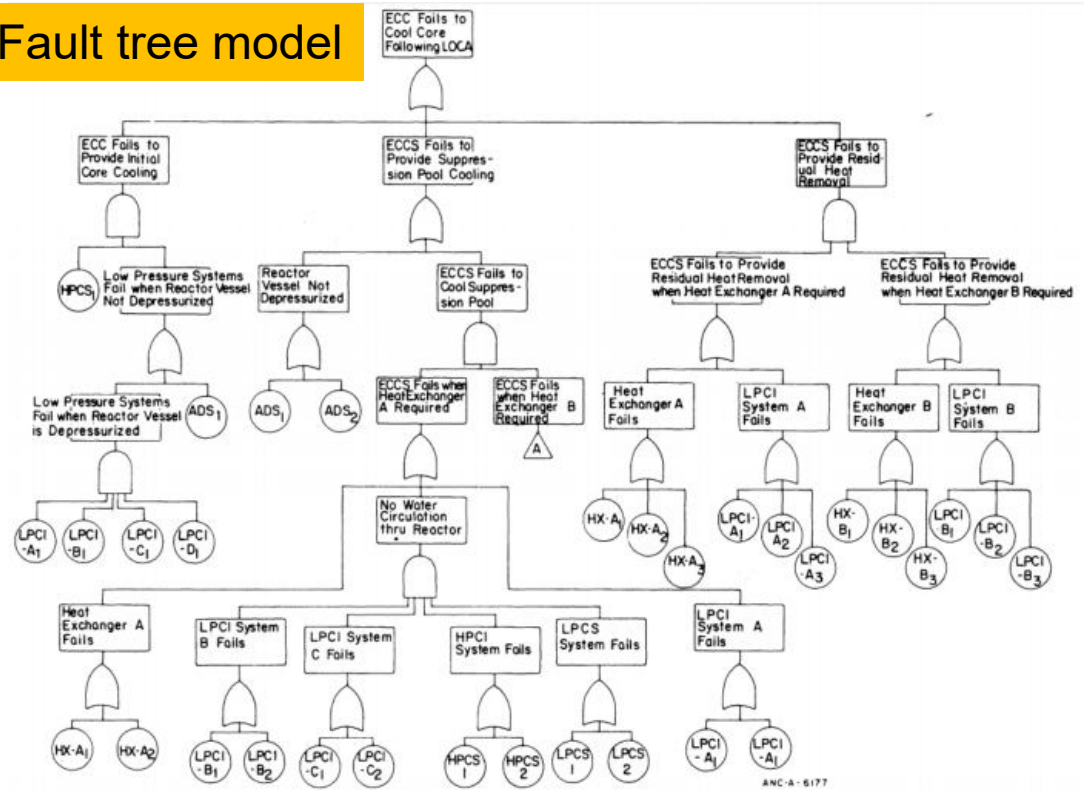
Case Example：ECCS



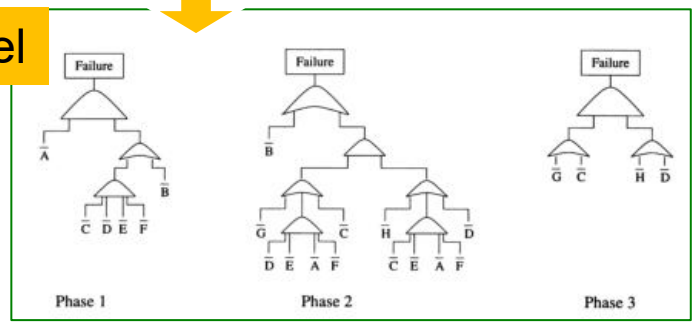
GO-FLOW Solver for Efficient Mission Reliability Analysis

☐ Case Study II: Emergency Core Cooling System

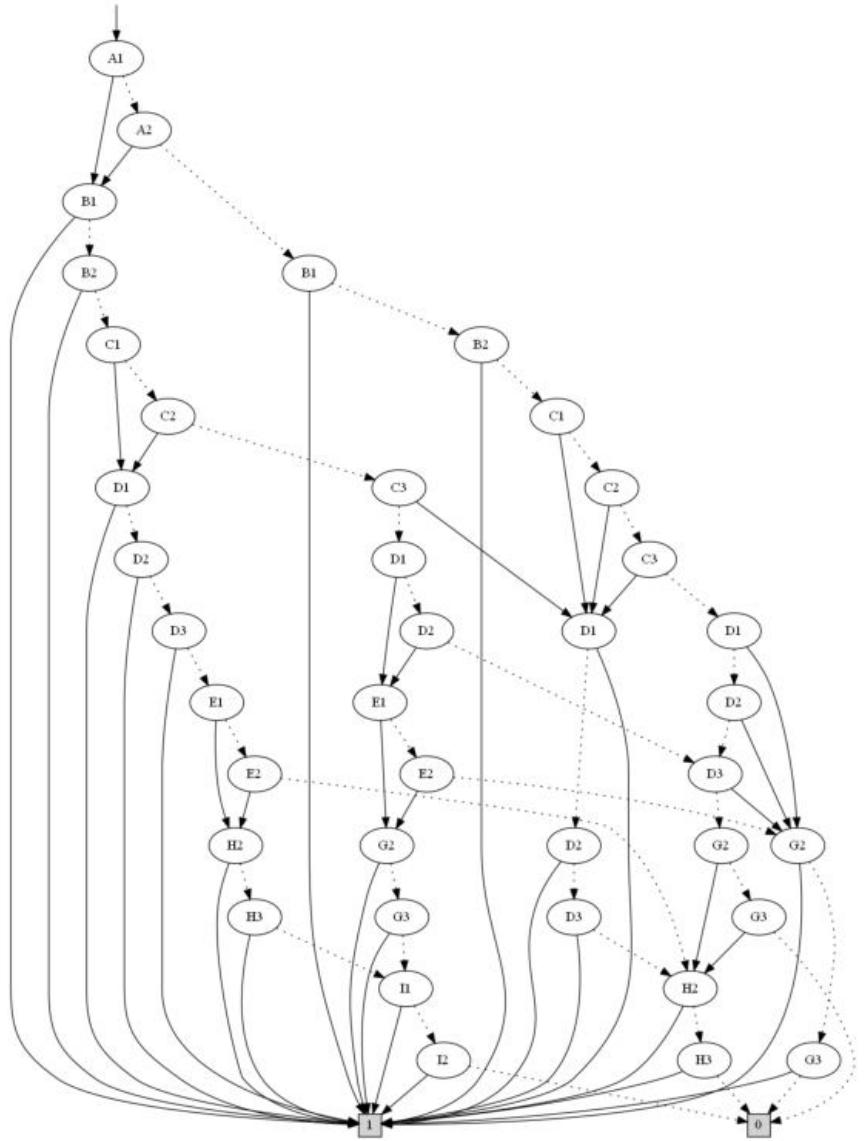
Fault tree model



Simplified FT model



Binary Decision Diagram



GO-FLOW Solver for Efficient Mission Reliability Analysis

Case Study II: Emergency Core Cooling System

- Ideal signal calculation

$$I(t) = R(t) / S(t)$$

$$\begin{cases} R(t) = 1.0 & (t < t_i) \\ R(t) = S(t) & (t_i \le t \le t_j) \\ R(t) = S(t_j) & (t_j < t) \end{cases}$$

- Independent signal merging and decomposition

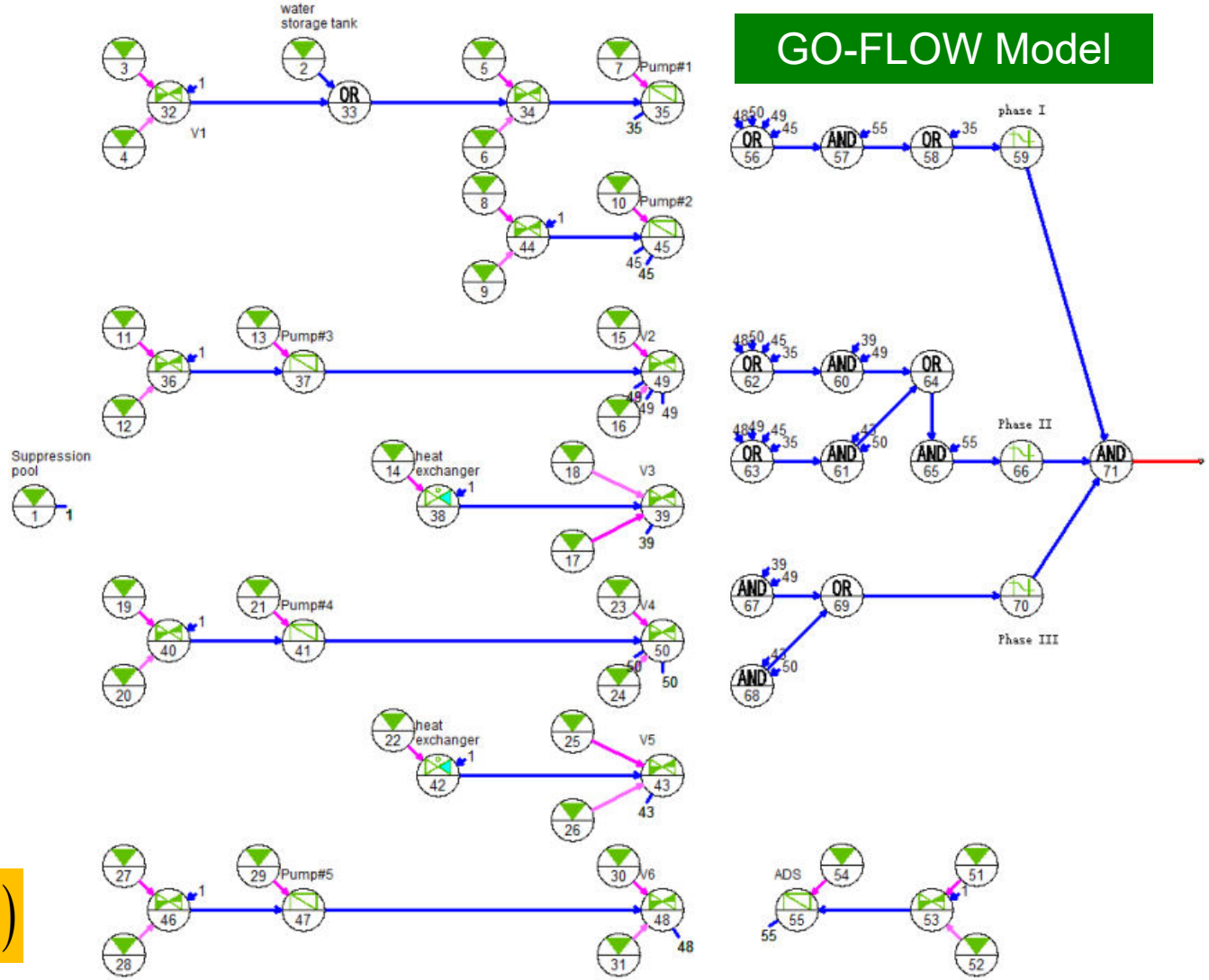
$$I'(t) = \max\left[I_1(t), I_2(t)\right]$$

$$\begin{aligned} I_1(t) &= I'(t) \\ I_2(t) &= I'(t) \cdot I''(t) \\ I_3(t) &= I'(t) \cdot I''(t) \cdot I'''(t) \end{aligned}$$

- Total probability decomposition of repeated signal

$$P(MPSs) = P\left(MPSs^1 \middle| S\right) \cdot P(S) + P\left(MPSs^0 \middle| \overline{S}\right) \cdot P\left(\overline{S}\right)$$

GO-FLOW Model



GO-FLOW Solver for Efficient Mission Reliability Analysis

■Analysis Results

The comparative analysis results [5] show that both the SDP (Sum of Disjoint Products)-based fault tree analysis, BDD, and the optimized GO-FLOW algorithm can provide exact solutions to the phased mission systems. The number of the minimal path sets to be processed by GO-FLOW is significantly less than the minimal cut sets in the fault tree analysis. The calculation efficiency is much more improved by the optimized GO-FLOW solver.

Method	System Failure Probability
GO-FLOW package	$5.22039 * 10^{-4}$
GFA	$5.220387349066 * 10^{-4}$
BDD	$5.220387349066 * 10^{-4}$
SDPP	$5.22038735 * 10^{-4}$

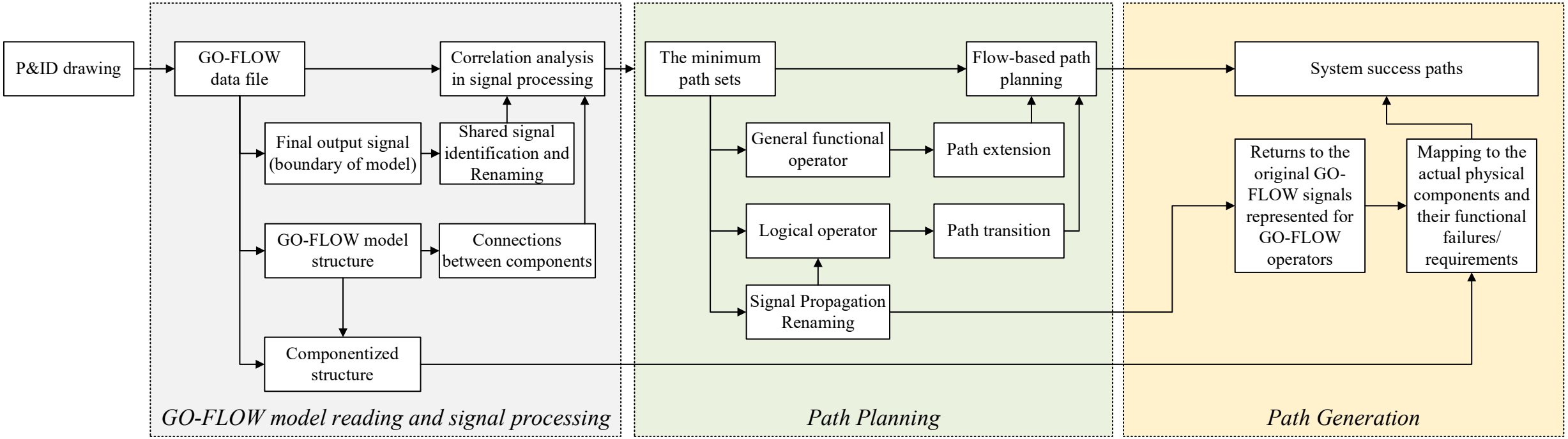
Method	MCS/MPS	Number
BDD	Disjoint minimal cut sets	145
	Minimal cut sets	59
GO-FLOW	Minimal path sets	80 (**8**)

Part III: Task and Success Path Planning for Emergency Response Management

☑ III-1: A Flow-directed MPSs Method for Success Path Planning[6]

The success path tracing and planning algorithm is implemented based on the inputs of complete set of ***minimal path sets*** that are obtained using graph traversal analysis on the GO-FLOW chart.

The success paths converted from minimal path sets can provide **procedural guidance from the perspective of function realization and goal achievement in a high level of abstraction**. The needs of step-by-step guide in temporal sequence are also considered with the sequential flow of signals, process simulation as well as practical engineering experiences in our ongoing studies.



Part III: Task and Success Path Planning for Emergency Response Management

III-1 A Flow-directed MPS Method for Success Path Planning

- The success path planning is implemented based on interpretation of minimal path sets, which are obtained from graph-based search analysis along with renaming of ideal signals of GO-FLOW operators.

Case Example: **PWR-AFWS**

Success Path-1: MPS {1, 6, 7, 8, 9, 10, 21}

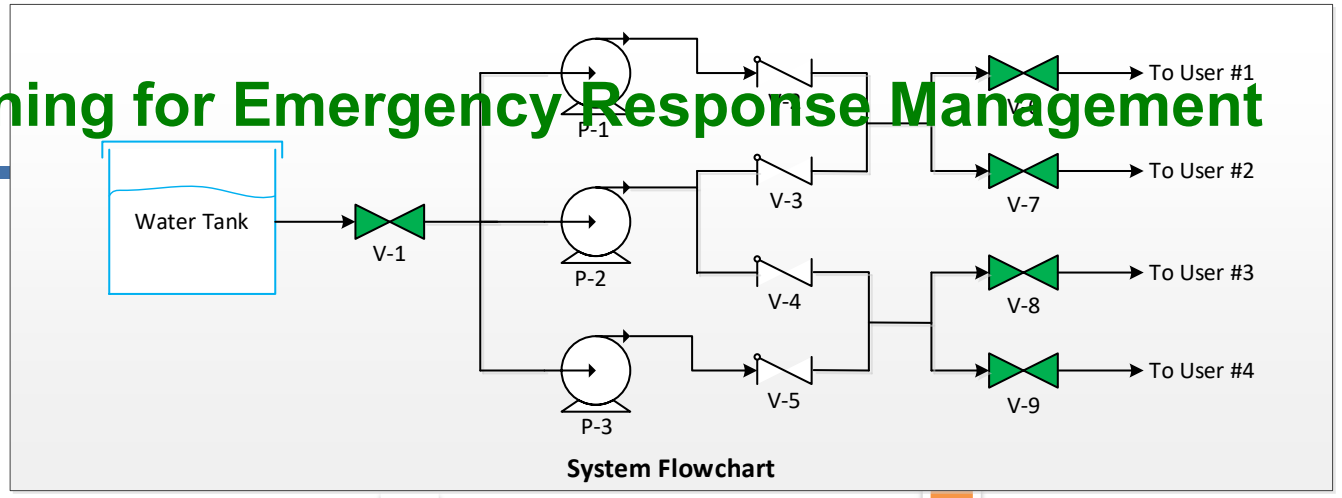
P(Success Path-1)=0.993400

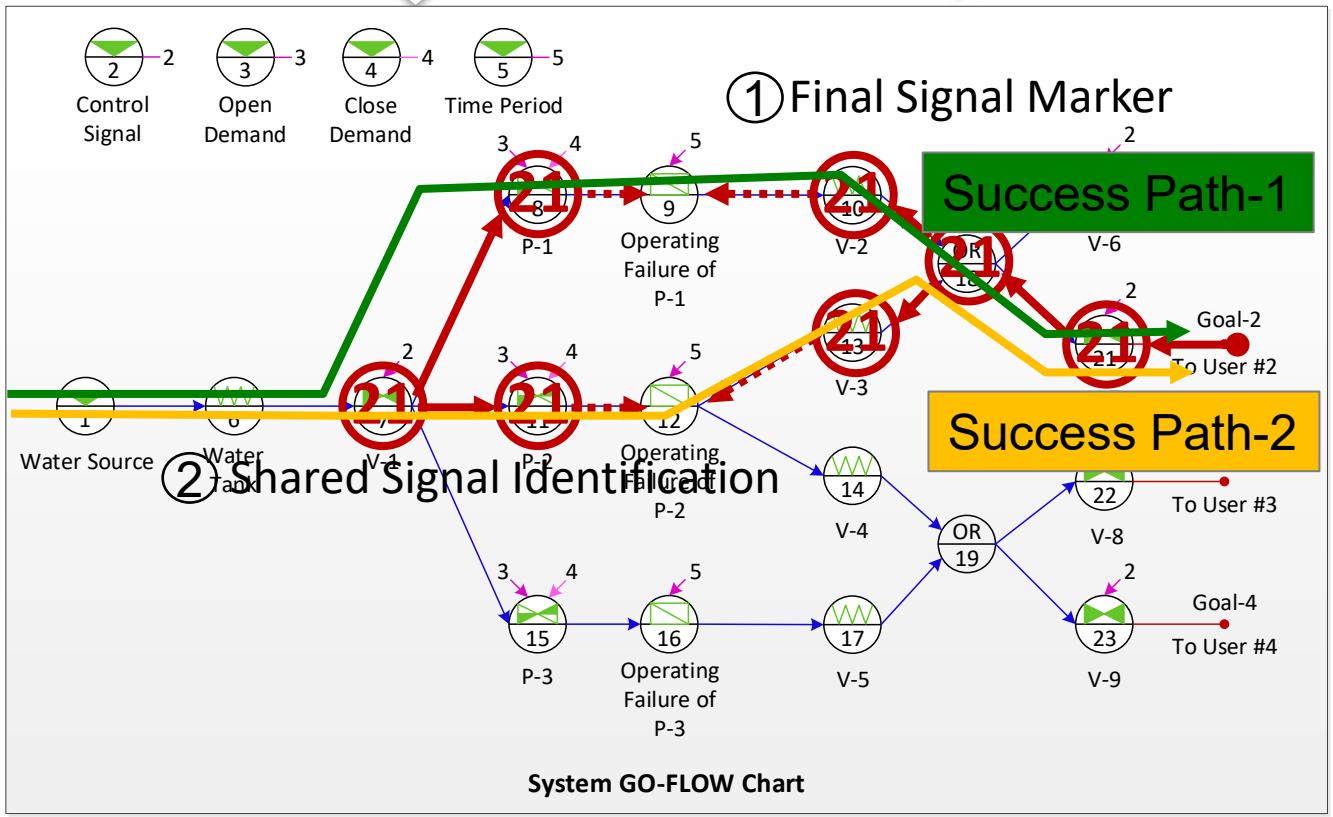
{Water tank with water, Open Valve V-1, Open Pump P-1, Keep P-1 operation for 2 hours, Open Valve V-2, Open Valve V-7}

Success Path-2: MPS {1, 6, 7, 11, 12, 13, 21}

P(Success Path-2)=0.0684003

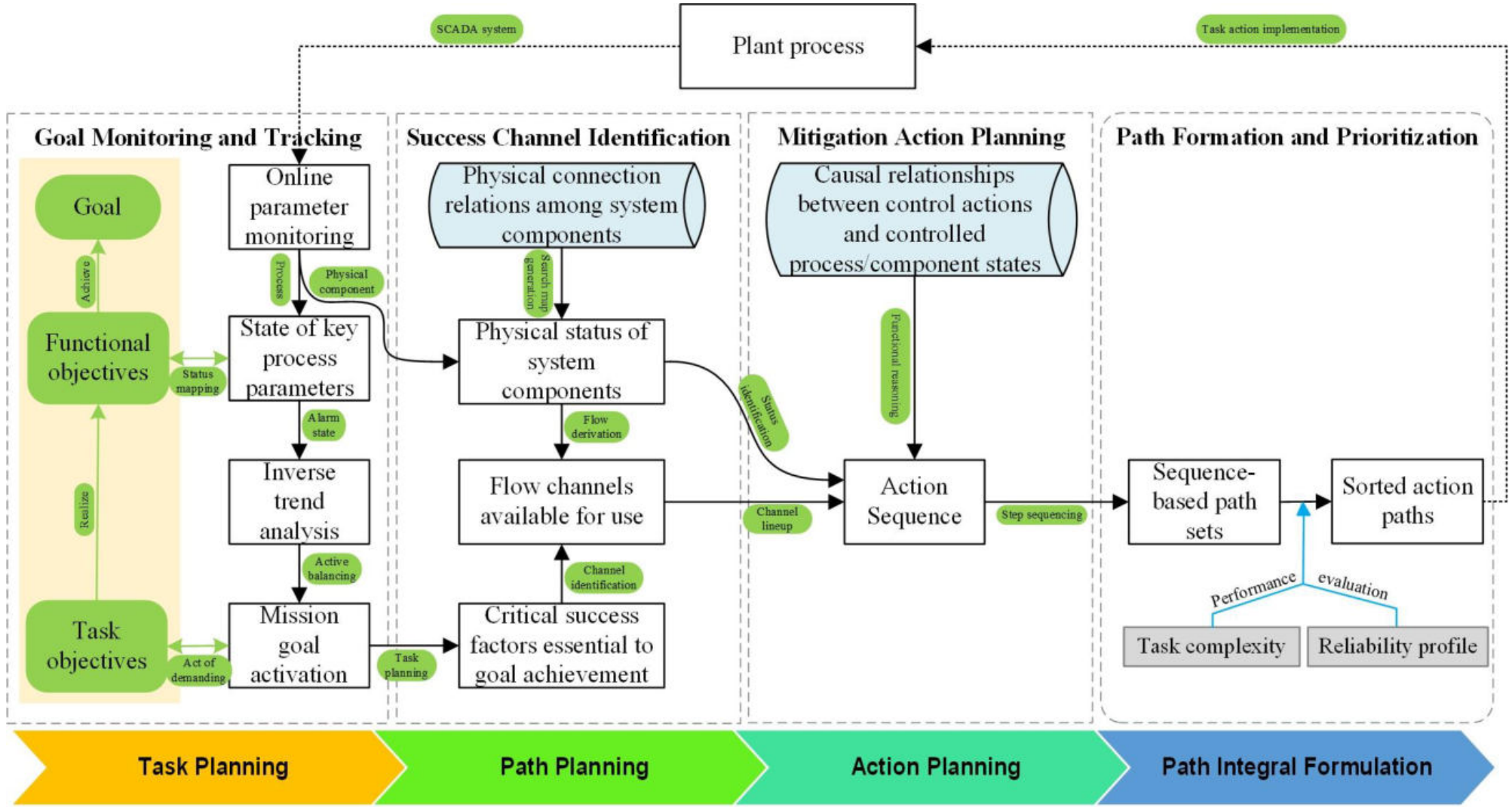
{Water tank with water, Open Valve V-1, Open Pump P-2, Keep P-2 operation for 2 hours, Open Valve V-3, Open Valve V-7}





Part III: Task and Success Path Planning for Emergency Response Management

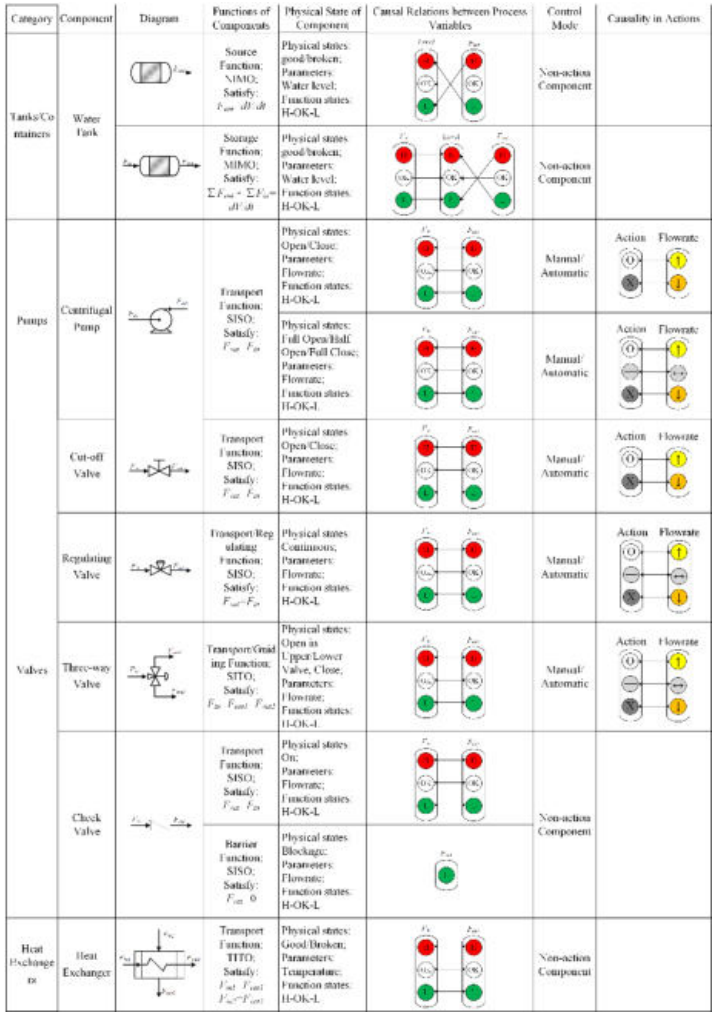
☑ III-2: Graph-based Emergency Countermeasure Planning[7]



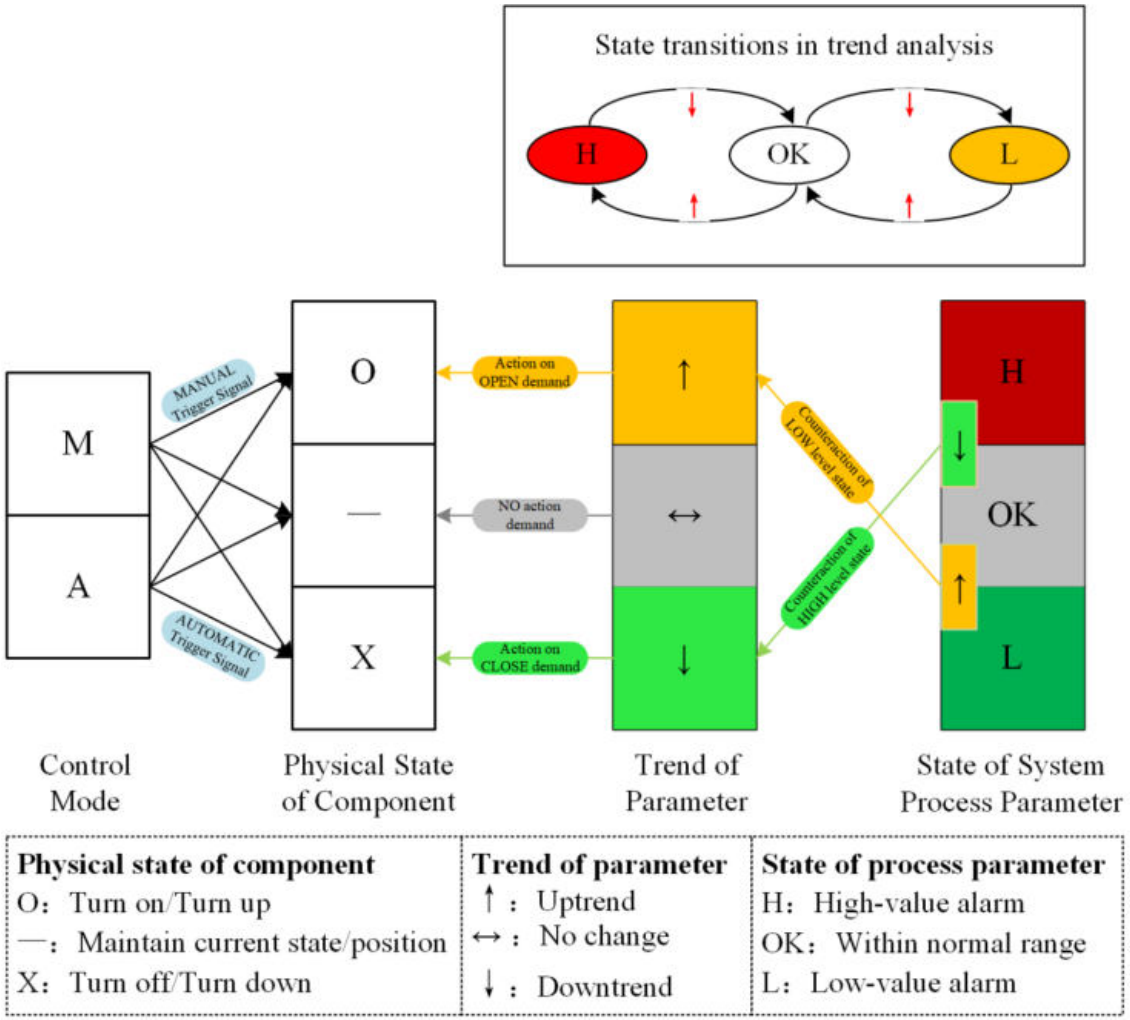
Part III: Success Path Planning for Emergency Response Management

☑ III-2: Graph-based Emergency Countermeasure Planning[7]

The emergency countermeasure planning method is implemented with goal- and function-oriented action formulization. The mission goal is determined based on system functional objectives and online monitoring of key process parameters (SPDS). The emergency action planning is carried out by ***deductive reasoning with anti-degradation goals and objectives in a reversed logical value setting***.



Knowledge Representation



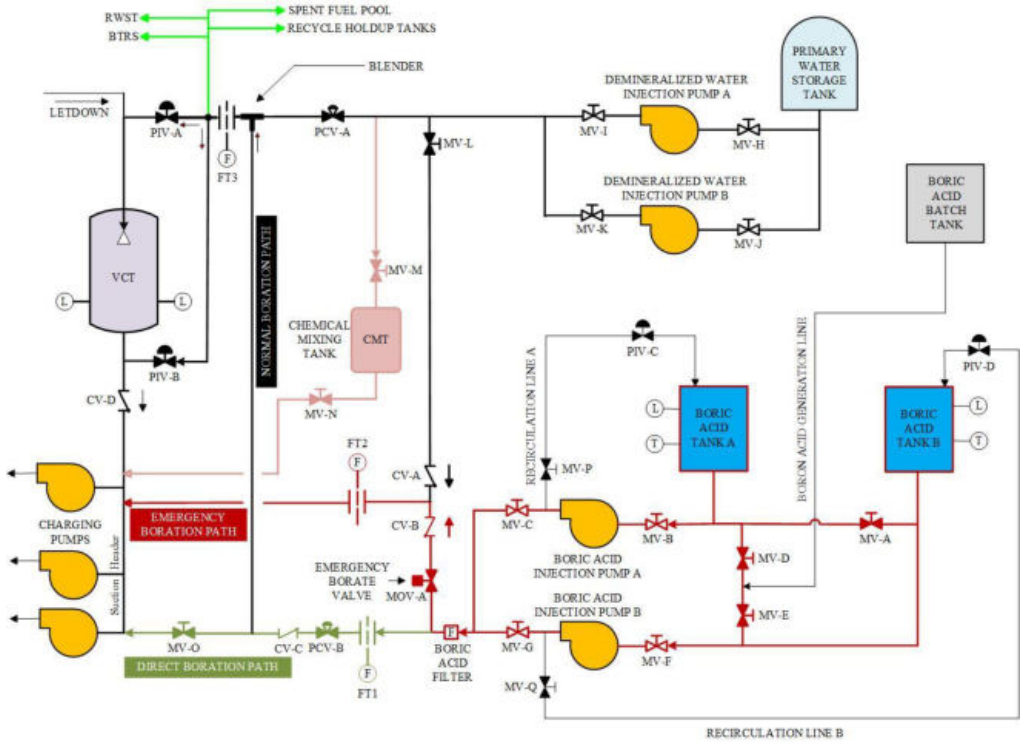
Backward Causation

Part III: Task and Success Path Planning for Emergency Response Management

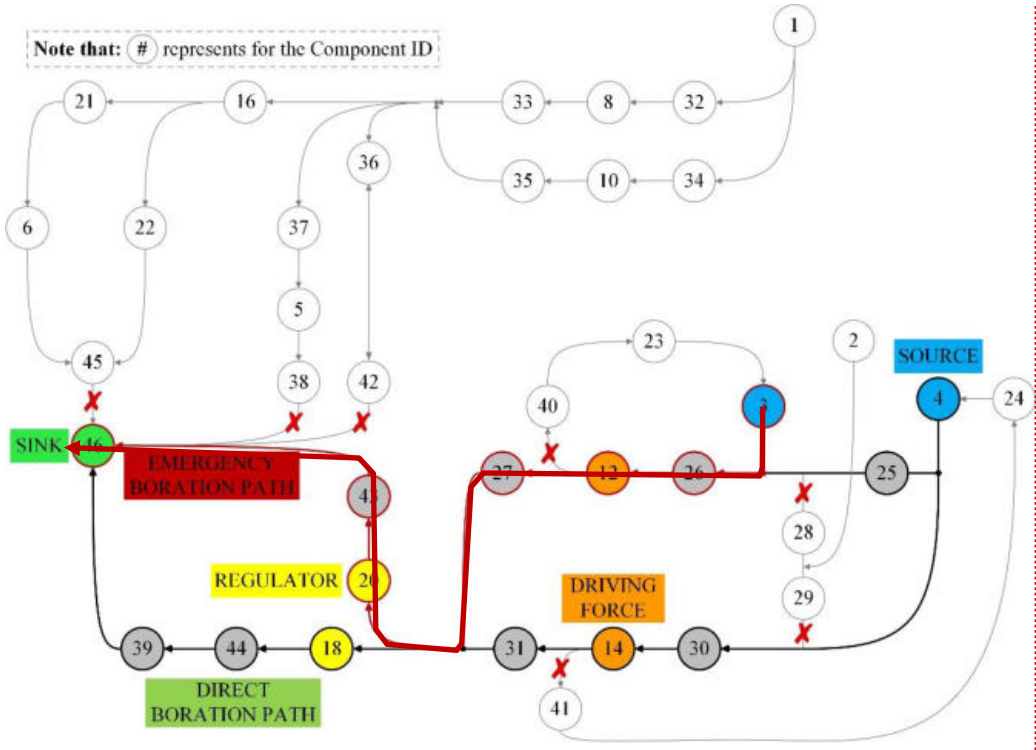
☑ III-2: Graph-based Emergency Countermeasure Planning[7]

Case Study: Manual Makeup under inadvertent boron dilution accident

For the specific mission objective derived from anomaly detection in process monitoring and controlling, the critical success factors essential to goal achievement are formulated in a form of functional organization of **{SOURCE + DRIVING FORCE + REGULATOR + SINK}.**



Reactor boron and water makeup system



Paths towards emergency boration recovery

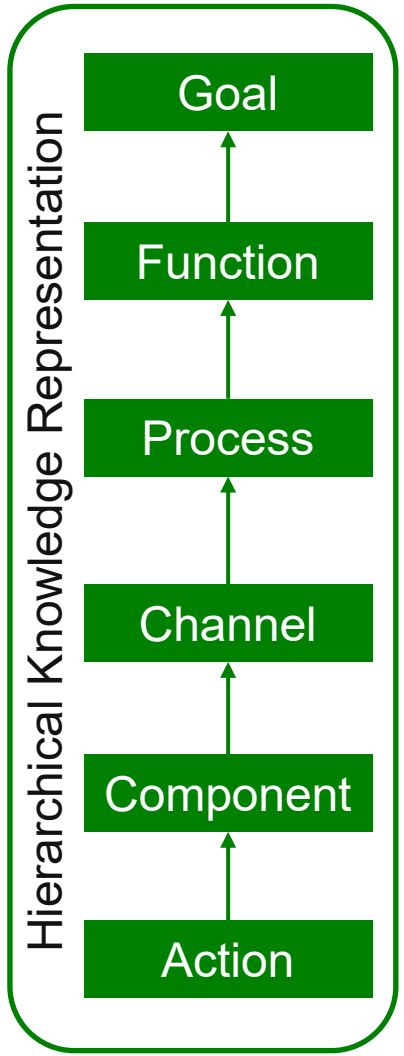
Action Sequence

- ☐ SelectMode@MANUAL
- ☐ Start@MANUAL
- ☐ SufficientContentsSupply@BAT-A
- ☐ Set@Flowrate
- ☐ MV-B@Open
- ☐ MV-C@Open
- ☐ Open@BAIP-A
- ☐ Open@MOV-A
- ☐ CV-B@ON
- ☐ ChargingLine@ON
- ☐ Stop@MANUAL

Part III: Task and Success Path Planning for Emergency Response Management

☑ III-3: MFM-based Emergency Countermeasure Planning

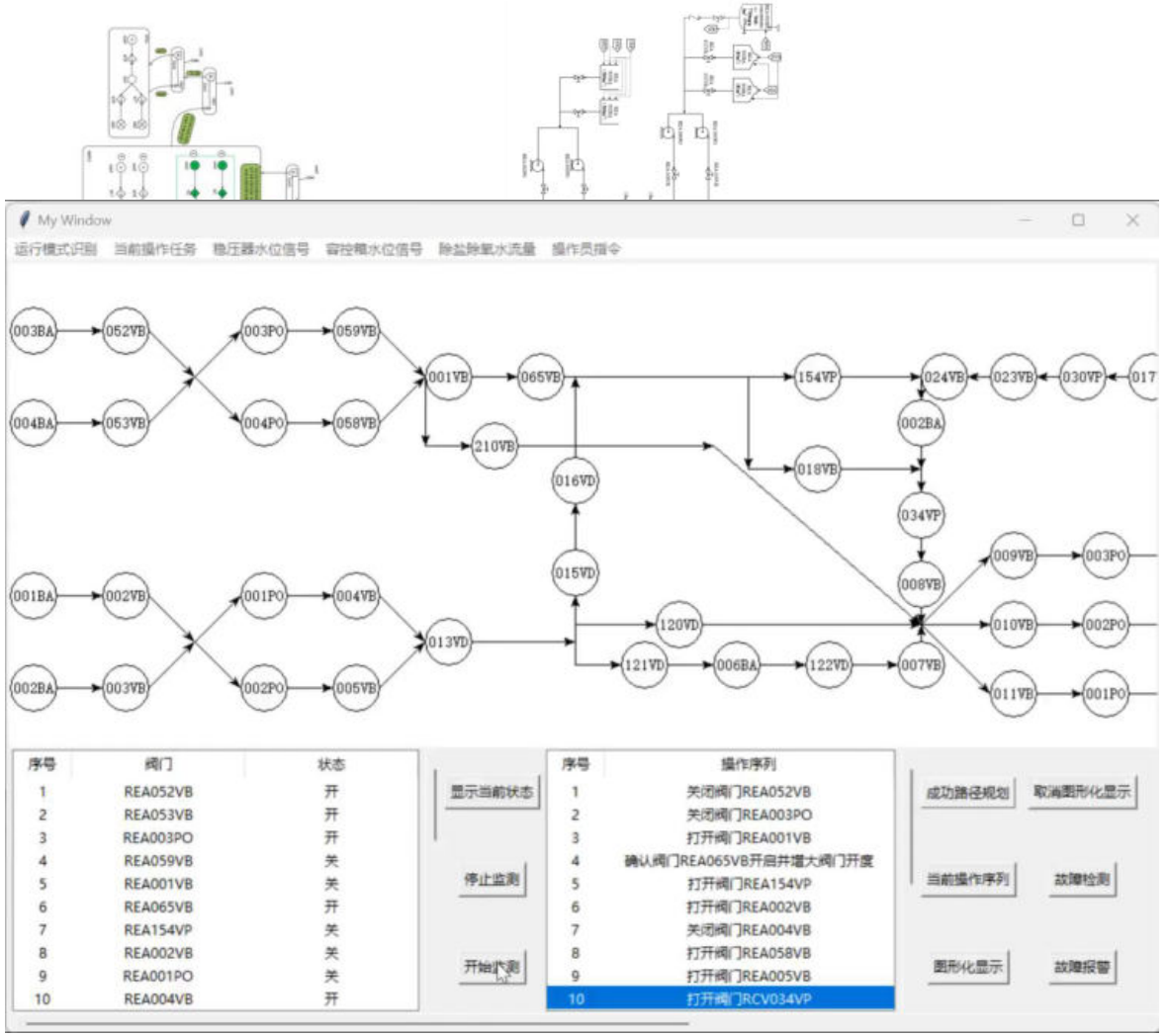
➢ **Emergency Countermeasure Planning based on MFM Process-oriented Reasoning**



Functional countermeasures and mitigation paths can be initiated through deductive reasoning of process parameters.

The routine function-behavior-structure MFM models are augmented with the control functions ***to explicitly describe the involved manual control and operation*** in a given task sequence.

Operational hazard analysis can also be carried out to proactively evaluate the hazard impact of anticipated operator actions onto plant safety based on MFM functional reasoning.



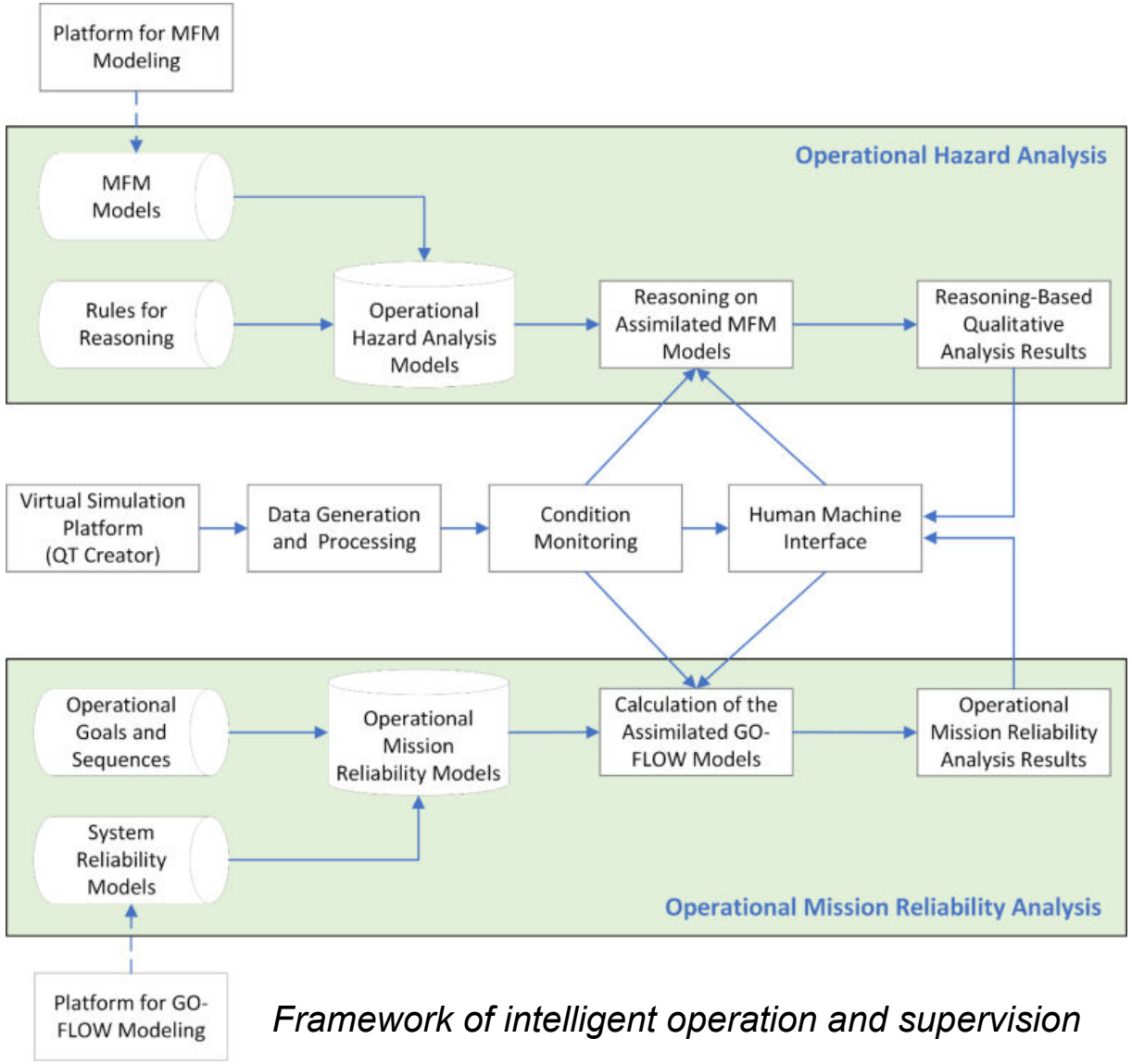
Part III: Task and Success Path Planning for Emergency Response Management

➢ Integrated Decision-Making Support System[8]

The integrated decision-making support system is designed to assistant operators in detecting, validating, identifying, diagnosing, assessing, monitoring, recovering from unsafe human actions in human-machine interactions in NPPs.

■ OBJECTIVES

- ☐ Uncovering the root causes and casual chains of problem
- ☑ Emergency response planning
- ☑ Operation navigation and supervision for task implementation
- ☐ Instantaneous hazard and reliability prediction
- ☑ Identification of underlying human error modes
- ☑ Proactive validation of operability of operators manual actions with necessary safety alerts
- ☐ Decision-making to redirect, recovery, and mitigate unsafe conditions

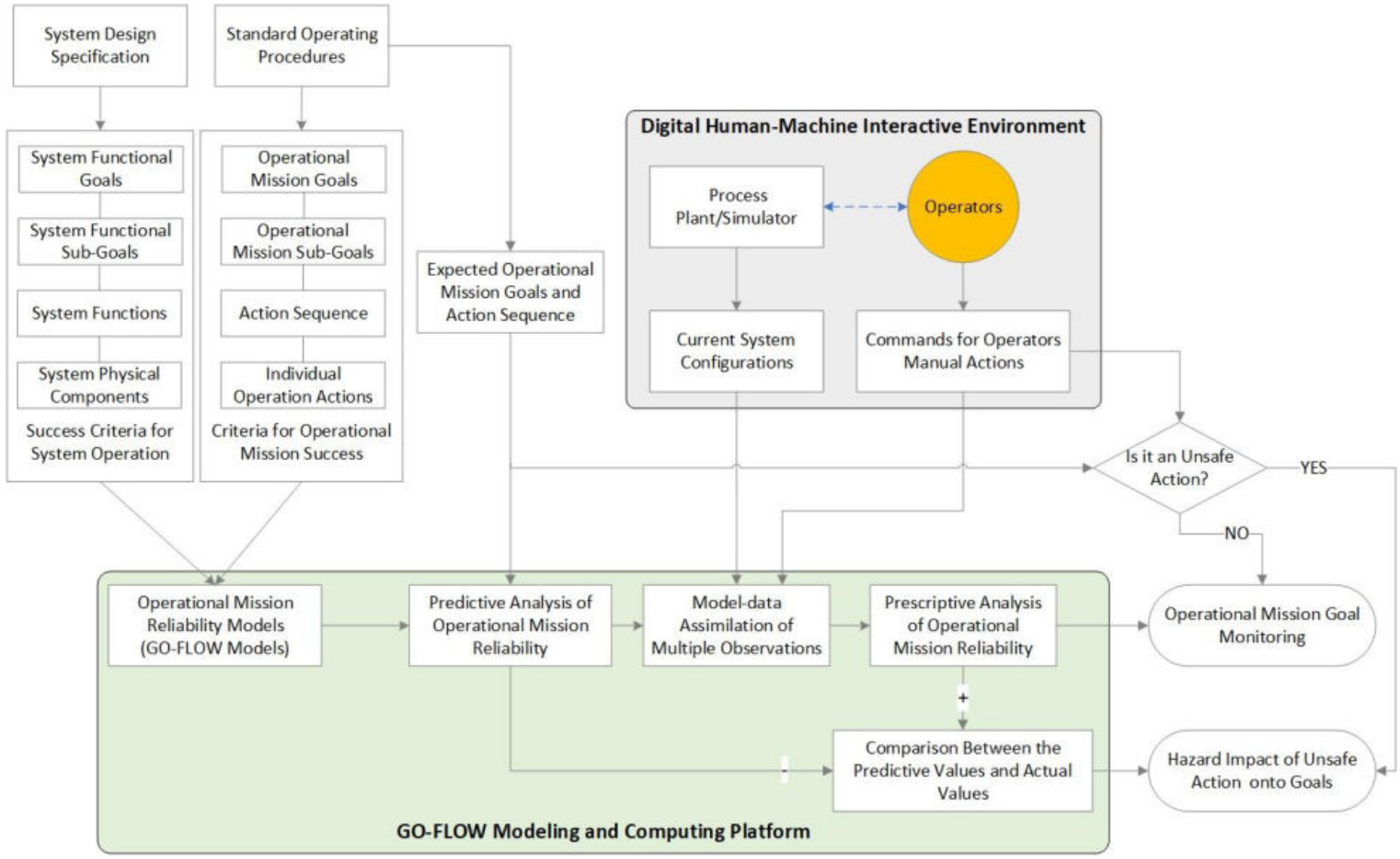


Framework of intelligent operation and supervision

Part III: Task and Success Path Planning for Emergency Response Management

☑ Operation Navigation and Supervision[8]

- The operation navigation and supervision involves **unsafe action identification**, **operational mission reliability analysis**, and ***tread impact analysis*** for task performance assessment.
- Pattern matching based supervision process is incorporated to intercept **unsafe actions** during task scheduling and implementation.
- The **operational mission reliability analysis** aims to quantitatively evaluate and map the operability of operators manual actions onto what extent the achievement of goals and objectives at all levels can be obtained for a given time period from a safety standpoint.
- The **tread impact analysis** is implemented based on synchronous prediction and supervision with mission reliability profile for hazard impact mapping.

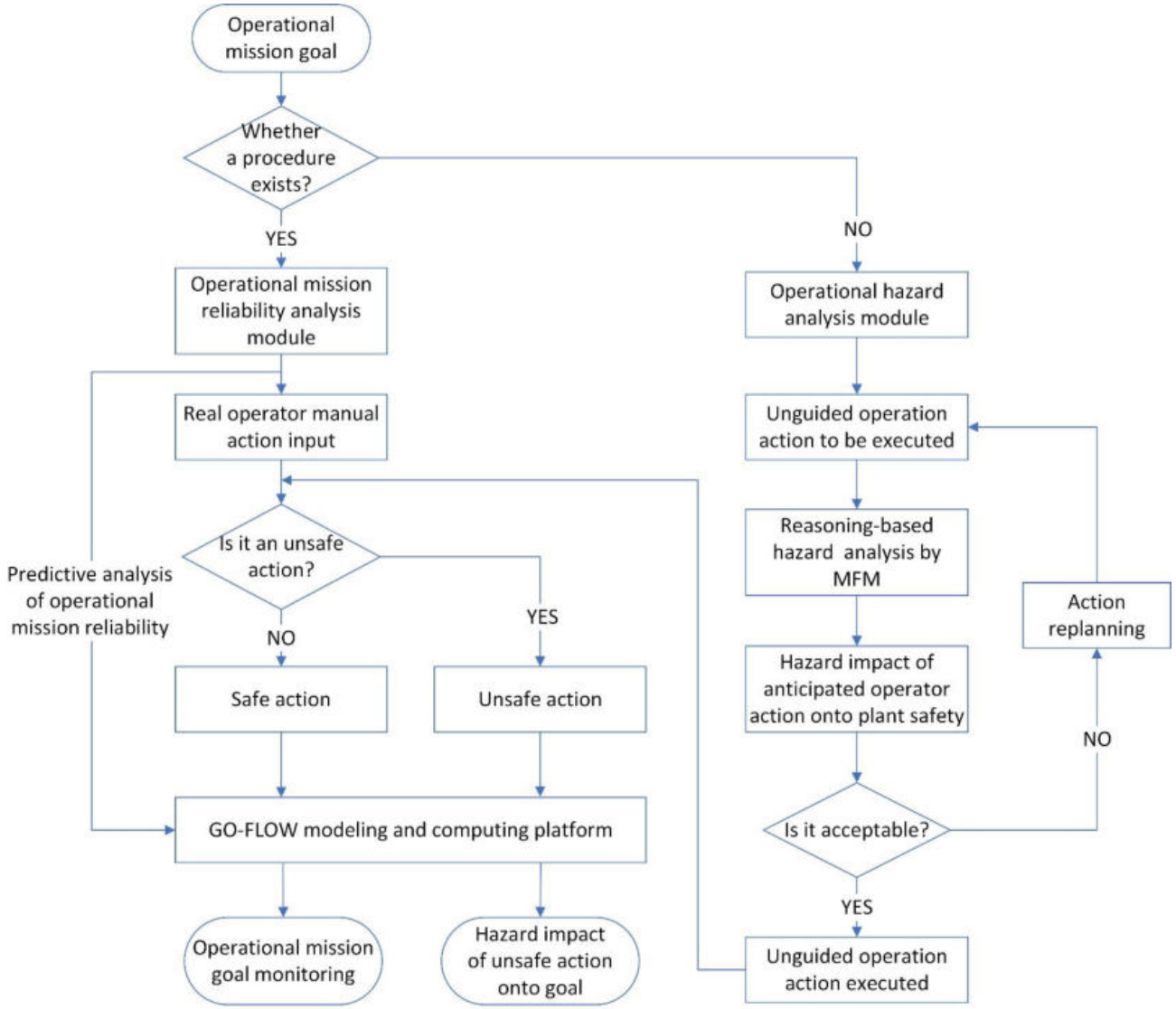


GO-FLOW modeling and analysis process for operational mission reliability analysis

Part III: Task and Success Path Planning for Emergency Response Management

Identification of Unsafe Action

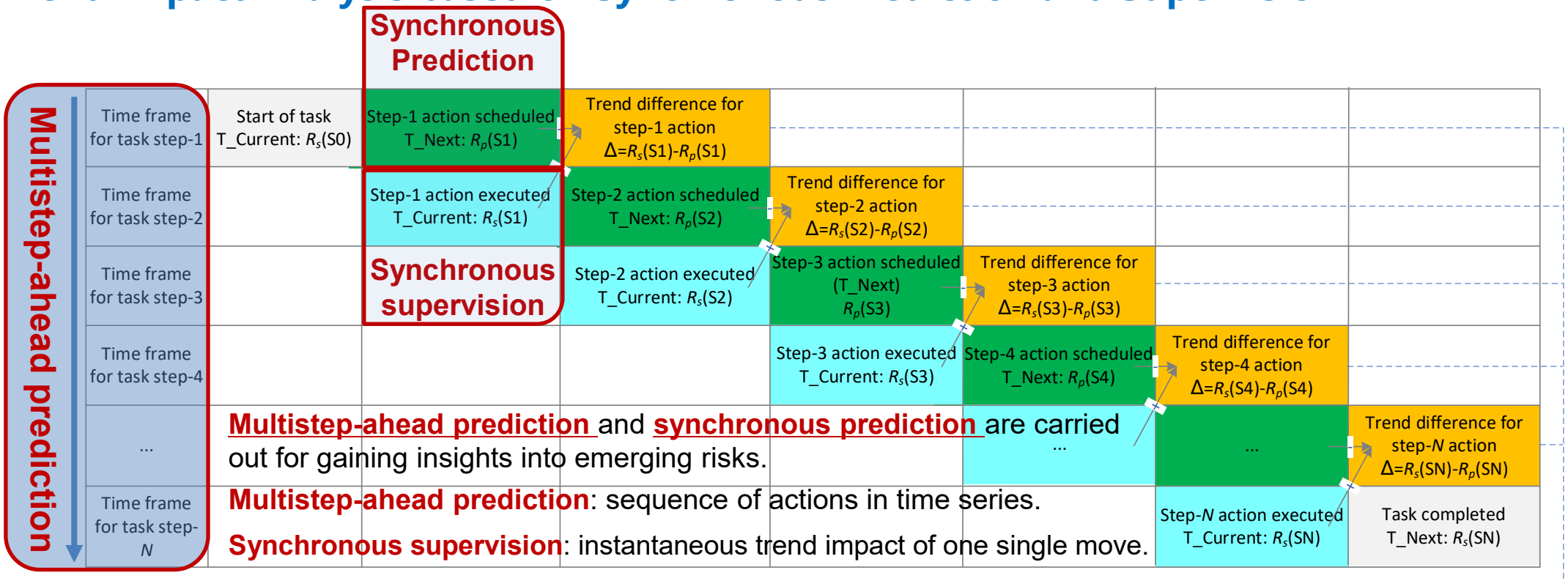
- The pattern matching-based supervision process starts with the operational mission goal, enters system operational scenario and intercepts operator actions during task scheduling.
- The actual operators manual actions executed in task implementation process are inputted into the procedural knowledge base for pattern recognition.
- The operators manual actions are inspected in accordance with the procedural knowledge base having due regard to ensuring the recognition of actions.
- **Without Procedure**: operational hazard analysis is carried out to proactively evaluate the hazard impact of anticipated operator actions onto plant safety based on functional reasoning.
- **With Procedure**: operational mission reliability analysis is performed to quantitatively evaluate the extent of impact of executed action on mission goal achievement by GO-FLOW.



Pattern-matching algorithm for operation action mode identification

Part III: Task and Success Path Planning for Emergency Response Management

Trend Impact Analysis based on Synchronous Prediction and Supervision



The impact trend is reflected by the difference between synchronous prediction and supervision, by which the underlying problems related to system abnormal operation or potential human errors can be mapped out. The size of difference in part reflects the criticality importance of a single step to the overall task success by including the human impact and contribution to overall system performance.

Input to Trend Impact Analysis		
Cases	Difference between synchronous supervision and prediction (Δ)	Impact trend
i	Δ=0	No effect for now
ii	Δ>0	Positive effects
iii	Δ<0	Negative effects

Part III: Task and Success Path Planning for Emergency Response Management

Reliability Profiler for Goal Monitoring

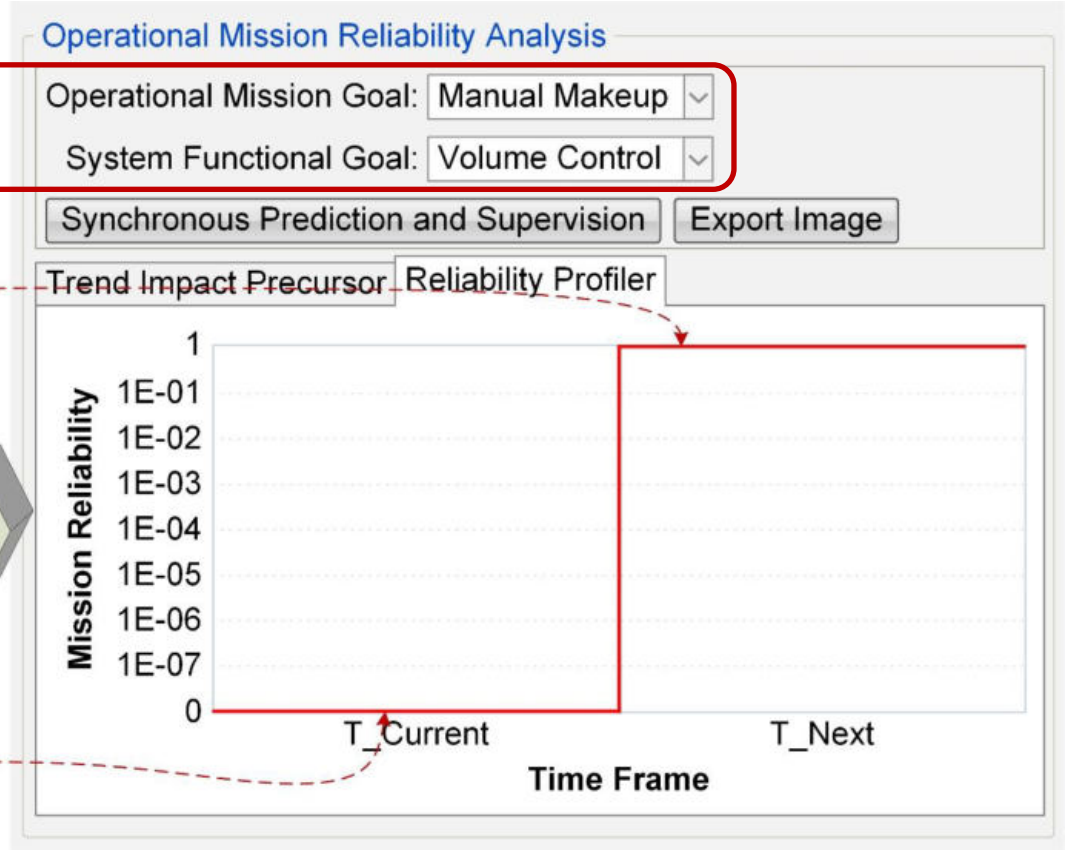
Trend impact precursor: provide a direct presentation of the results of the synchronous prediction and supervision analyses by intuitive.

Reliability profiler: a mission profile-based visualization of time-oriented data obtained in each task step.

Support for multi-goal monitoring

Trend Impact Precursor | Reliability Profiler

Action Step	Synchronous Prediction	Synchronous Supervision	Trend Difference	Safety Alerts
S1	0	0	0	No Effect for Now
S2	0	0	0	No Effect for Now
S3	0	0	0	No Effect for Now
S4	0.99752948			

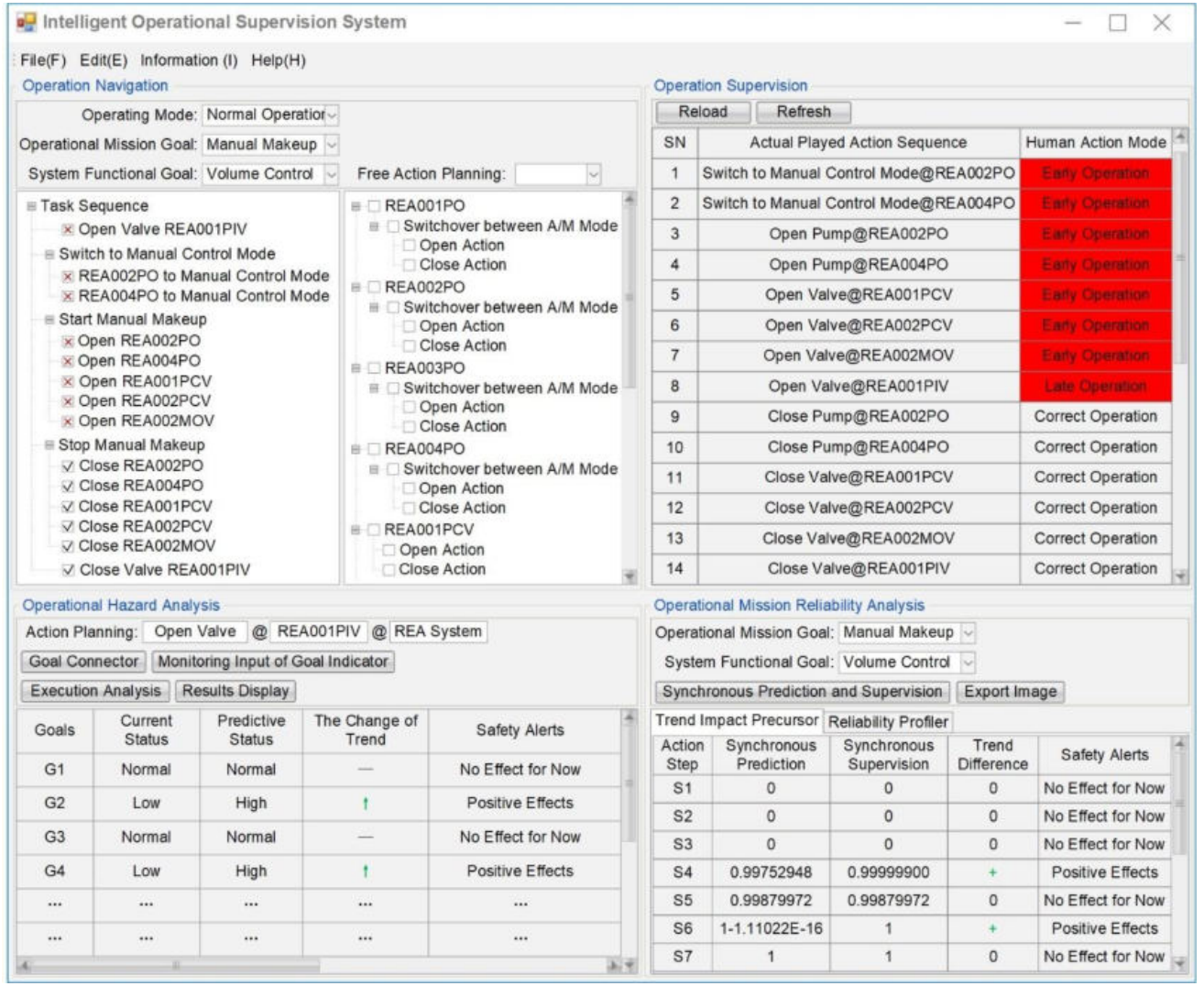


Part III: Task and Success Path Planning for Emergency Response Management

☑ Operation Navigation and Supervision[10]

An integrated decision-making support system is developed with the integration of following capabilities.

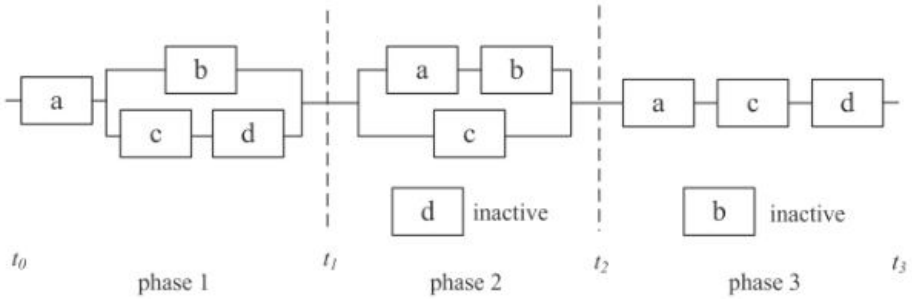
- Unsafe Action Identification (Pattern-matching)
- Procedure-based Navigation and Supervision
- Non-procedural Path Guiding
- Operational Mission Reliability Monitoring
- Trend Impact Prediction
- ☒ **Operational Hazard Analysis (Based on inductive reasoning analysis)**



FUTURE WORKS

☐ Expansion and Optimization of GO-FLOW Platform

(1) Reliability analysis of repairable PMS system

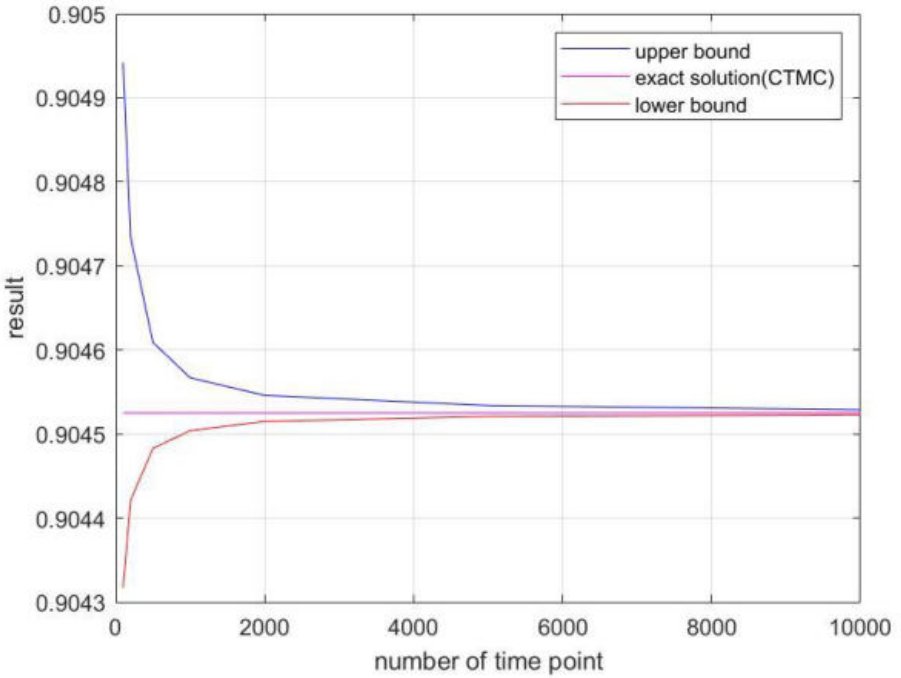


Essential problems to be solved:

① Exact solution of availability of repairable PMS system (Continuous-Time Markov Chain, CTMC)

② Balance efficiency, accuracy, and flexibility in system reliability/availability calculation. (GO-FLOW/Markov chain with flexible time point interpolation)

③ Obtain margin of error, confidence interval, confidence level.



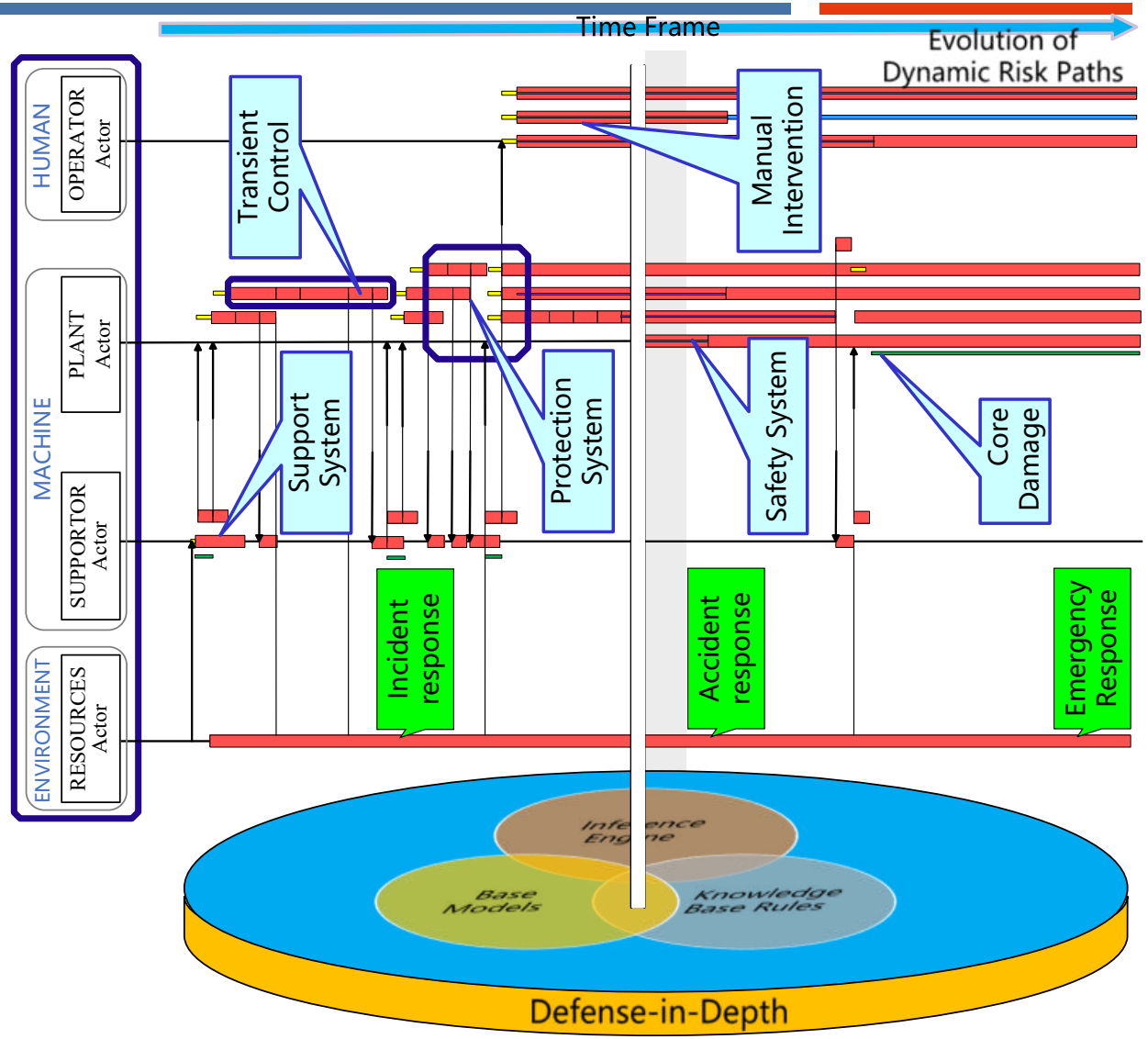
FUTURE WORKS

Defense-in-Depth Nuclear Safety and Emergency Risk Management Platform

It is committed to providing a multi-layered integration framework to preventing accidents from happening and to mitigate their consequences from the Layer 1 of PREVENTION to Layer 5 of Emergency Response. The following functional modules will be focused in our future studies:

- Supervisory control of critical safety functions based on the Three C' s principles (CONTROL-COOL-CONTAIN).
- Emergency Countermeasure Planning for Functional Recovery and Hazard Mitigation
- Optimal Allocation of Emergency Resources

https://medium.com/@6unpnp/defence-in-depth-an-intro-fe6e1b86f5db



References

[1] Zhanyu He, Jun Yang, Takeshi Matsuoka, et al. An automated GO-FLOW modeling tool for system reliability analysis. Proceedings of the 30th International Conference on Nuclear Engineering (ICONE30), May 21-26, 2023.

[2] Zhanyu He, Jun Yang, Yongyue Chu. A synthesis component-based GO-FLOW modeling paradigm for automated time-dependent and phased-mission reliability model generation and analysis. IEEE Transactions on Reliability, 2024. (Under review)

[3] Licheng Zheng, Xinyu Dai, Jun Yang, et al. A flexible optimization algorithm for GO-FLOW methodology to deal with shared signals. Annals of Nuclear Energy. 156(108200): 1-15, 2020.

[4] Chenyu Jiang, Zhanyu He, Fengjun Li, et al. A hybrid computing framework for risk-oriented reliability analysis in dynamic PSA context: a case study. Quality and Reliability Engineering International, Vol. 2022, pp. 1-27, 2022.

[5] Zhanyu He, Jun Yang, Takeshi Matsuoka, et al. Reliability analysis of phased mission systems using GO-FLOW methodology. ICONE29, August 8-12, 2022.

[6] Zhanyu He, Jun Yang, Yueming Hong. A flow-directed minimal path sets method for success path planning and performance analysis. Nuclear Engineering and Technology, 2023.

[7] Jun Yang, Yueming Hong, You Xue, Shuxin Bi, Wenlin Wang. A goal-oriented emergency countermeasure planning method using graph-based path search and functional reasoning. Progress of Nuclear Energy, 170: 105109, 2023.

[8] Jun Yang, You Xue, Xinyu Dai, Hongxin Lu, Ming Yang. An intelligent operational supervision system for operability and reliability analysis of operators manual actions in task implementation. Process Safety and Environmental Protection. 158: 340-359, 2022.

Thank you for your time and attention.