TIMED-FAULT TREE GENERATION FROM DYNAMIC FLOWGRAPH METHOD

Chireuding Zeliang
Graduate Research Assistant
Faculty of Energy Systems and Nuclear Science
University of Ontario Institute of Technology
Oshawa, ON, Canada

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

26th Sept. 2017

OUTLINE

- Motivations
- System Description
- Dynamic Flowgraph Method
- Prime Implicants
- Timed-Fault Trees Generation
- Conclusions

Motivations

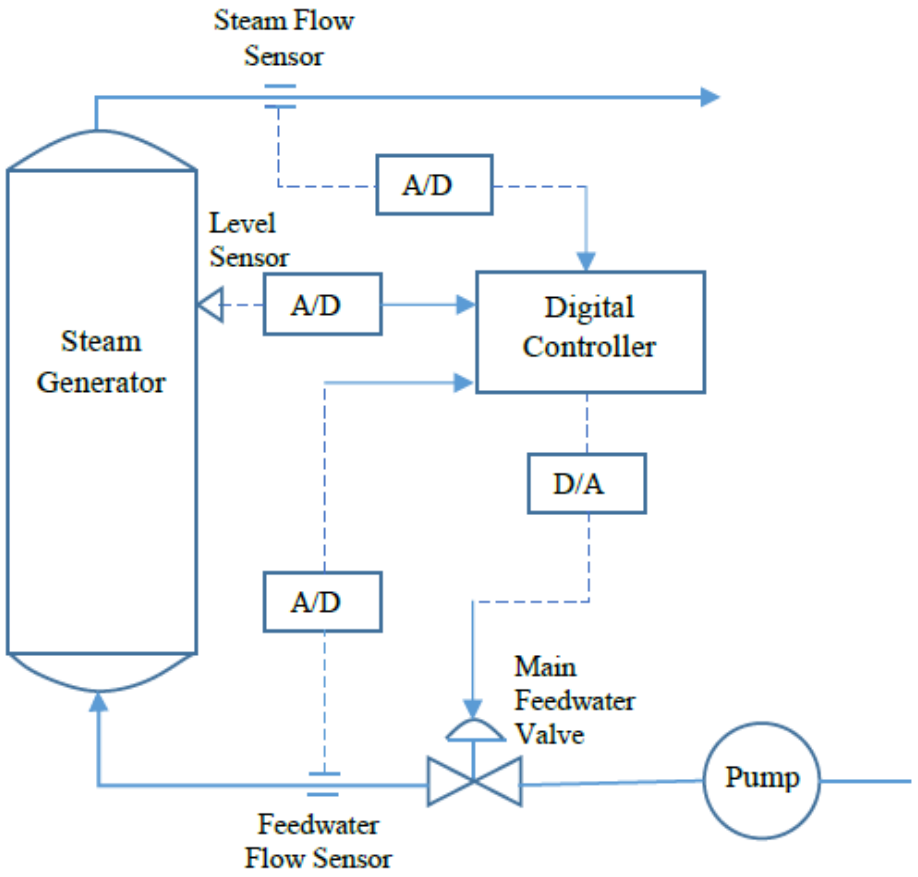
- Many new and old NPPs are intended to *upgrade or replace the aging control systems* from analogue to digital technology
- *Currently limited guidance and consensus* on reliability modelling of digital system
- *Integrated analysis* of Software and Hardware systems
- *Incorporation of Dynamic Models* into existing conventional PRA models

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

System Description

System Components:

1. U-tube Steam Generator
2. Feedwater Pump
3. Digital Controller
4. Main Feedwater Valve
5. Level Sensor
6. Feedwater Flow sensor
7. Steam Flow sensor
8. A/D converter
9. D/A converter



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

System Boundary Conditions

- A *Non-repairable* system

Physical Consistency:

- A process variable with different state cannot occur at the same time step (e.g., *valve open AND valve closed @t= -1 cannot happen*)

Dynamic Consistency:

- A process variable can change its states only by a certain amount in a single time-step (e.g., *SG level cannot change from 0% to 90% in a single time step*)

Dynamic Flowgraph Method?

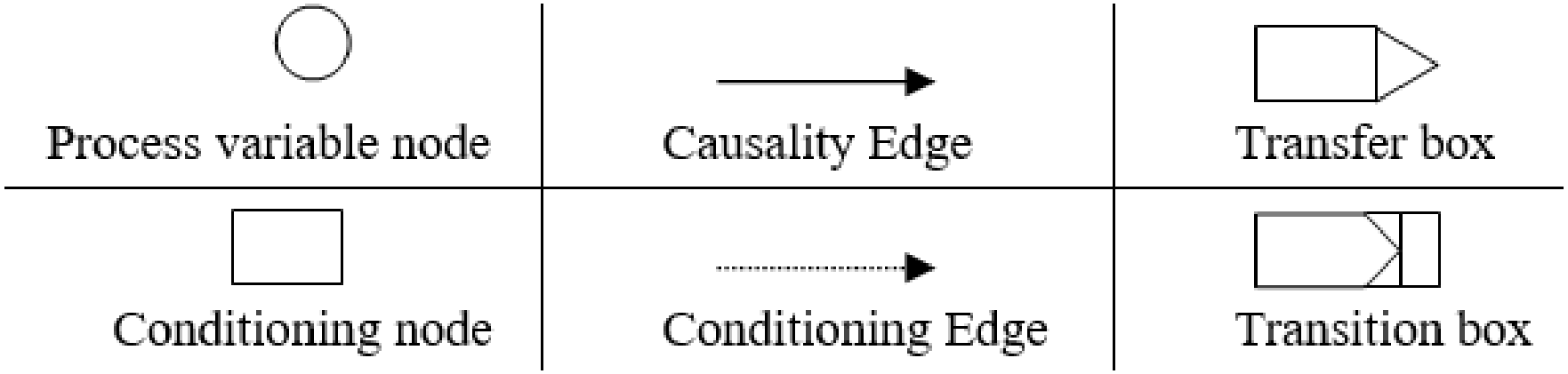
- The *IAEA and the USNRC* study ranked DFM an Markov-CCMT as the *top two* with most viable, positive features and least uncertain features for reliability analysis of digital systems *[NUREG-6901]*
- DFM can provide the multi-state and time-dependent *equivalent of both FTA and FMEA*
- A system approach to *Integrate hardware and software analysis*

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Dynamic Flowgraph Method

- A Multi-Valued Logic Model (*unlike binary states-0,1*) and non-coherent
- Expresses the logical and dynamic (*time-dependent*) behavior of a system
- Dynamic behaviors are represented as a *series of discrete state transitions*
- When did the failure event occurred? At what magnitude?

DFM modelling elements



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

DFM Modelling Approach

A two step Process:

1. Model construction (*DYMONDA*)
2. Model Analysis (*Inductive or Deductive*) – the latter is used in this paper.

Process Variable Discretization

- All Process Variables are discretized into arbitrary number of states *(analyst choice)*

SG Level Sensor state

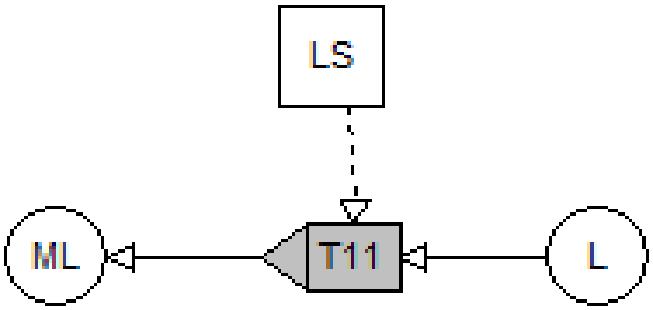
State	Description
-1	Failed Low
0	Normal
+1	Failed High

SG Level

State	Description
0	0% – 25%
1	25% - 50%
2	50% – 60%
3	60% – 70%
4	70% – 80%
5	80% – 85%
6	85% – 90%
7	90% – 100%

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Decision Table Development

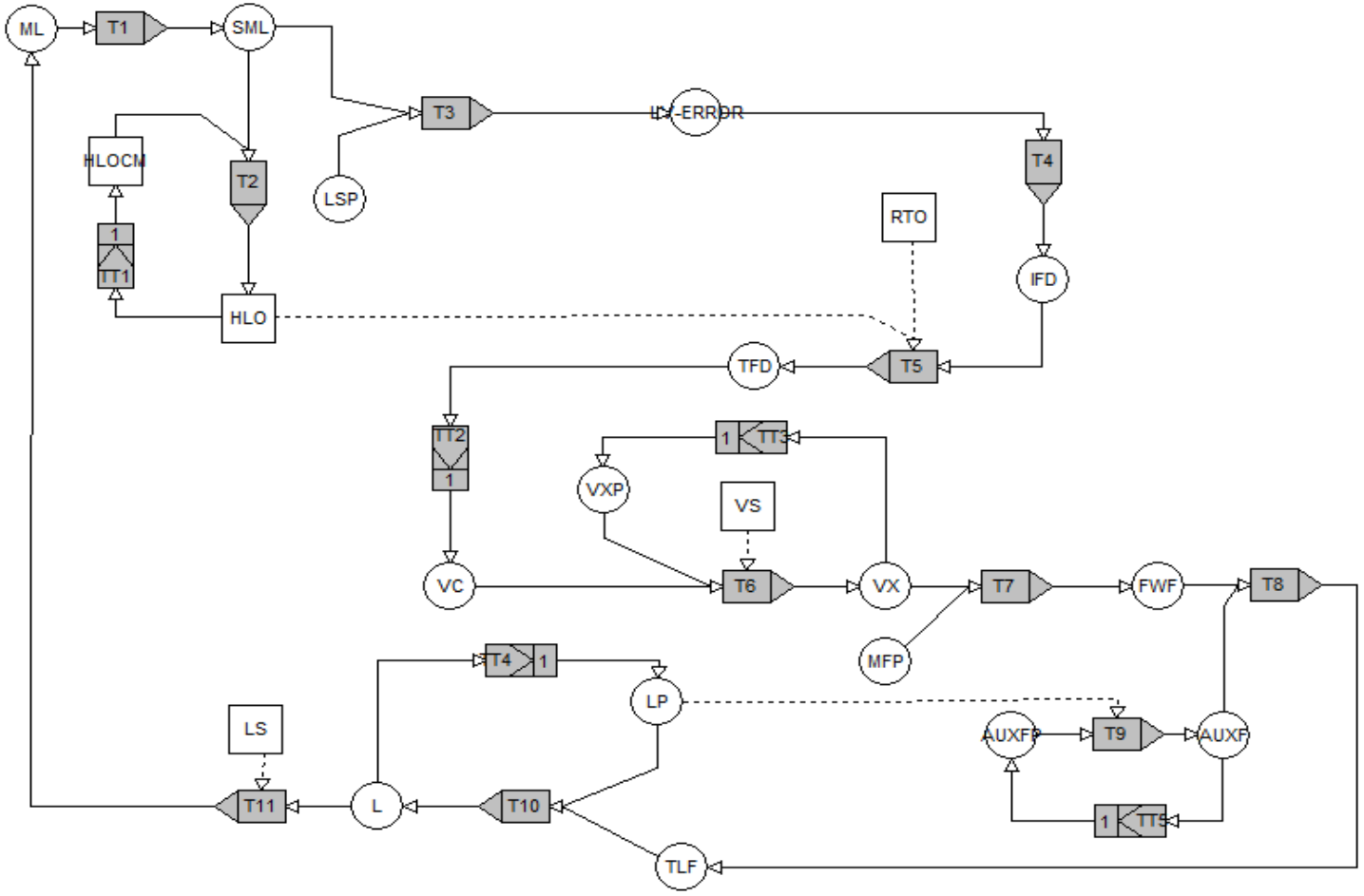


Decision table of T11

No.	LS	L	ML
1.	1	0	0
2.	1	1	1
3.	1	2	2
4.	1	3	3
5.	1	4	4
6.	1	5	5
7.	1	6	6
8.	1	7	7
9.	-1	*	0
10.	+1	*	7

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

DFM model of a 1-element SGLC system



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

26th Sept. 2017

Prime Implicants

- *Implicants:* Analogous to Cut-sets in FTA
- *Prime Implicants:* Analogous to Minimal cut-set in FTA, but it is *time-stamped* *(e.g., A_i@t=-1 : A variable "A" have state "i" at time "t=-1")*
- *Base:* Set of Prime implicants logically equivalent to the TOP function
- *Complete Base of Prime Implicants:* Identification by the *Method of Generalized Consensus*

Prime Implicants for SG Overflow

#	Prime Implicants	Time	Logic
1.	SG level was between 90% to 100%	@t= -1	
2.	Main feed pump is normal	@t=0	AND
	Main feed valve stucked high	@t=0	AND
	SG level was between 85% to 90%	@t= -1	
3.	Main feed pump is normal	@t=0	AND
	Main feed valve is normal	@t=0	AND
	Reactor trip override signal was inactive	@t= -1	AND
	High level override signal was inactive	@t= -1	AND
	SG level sensor stucked low	@t= -1	AND
	SG level was between 85% to 90%	@t= -1	AND
	Main feed valve was open between 60% to 80%	@t= -1	

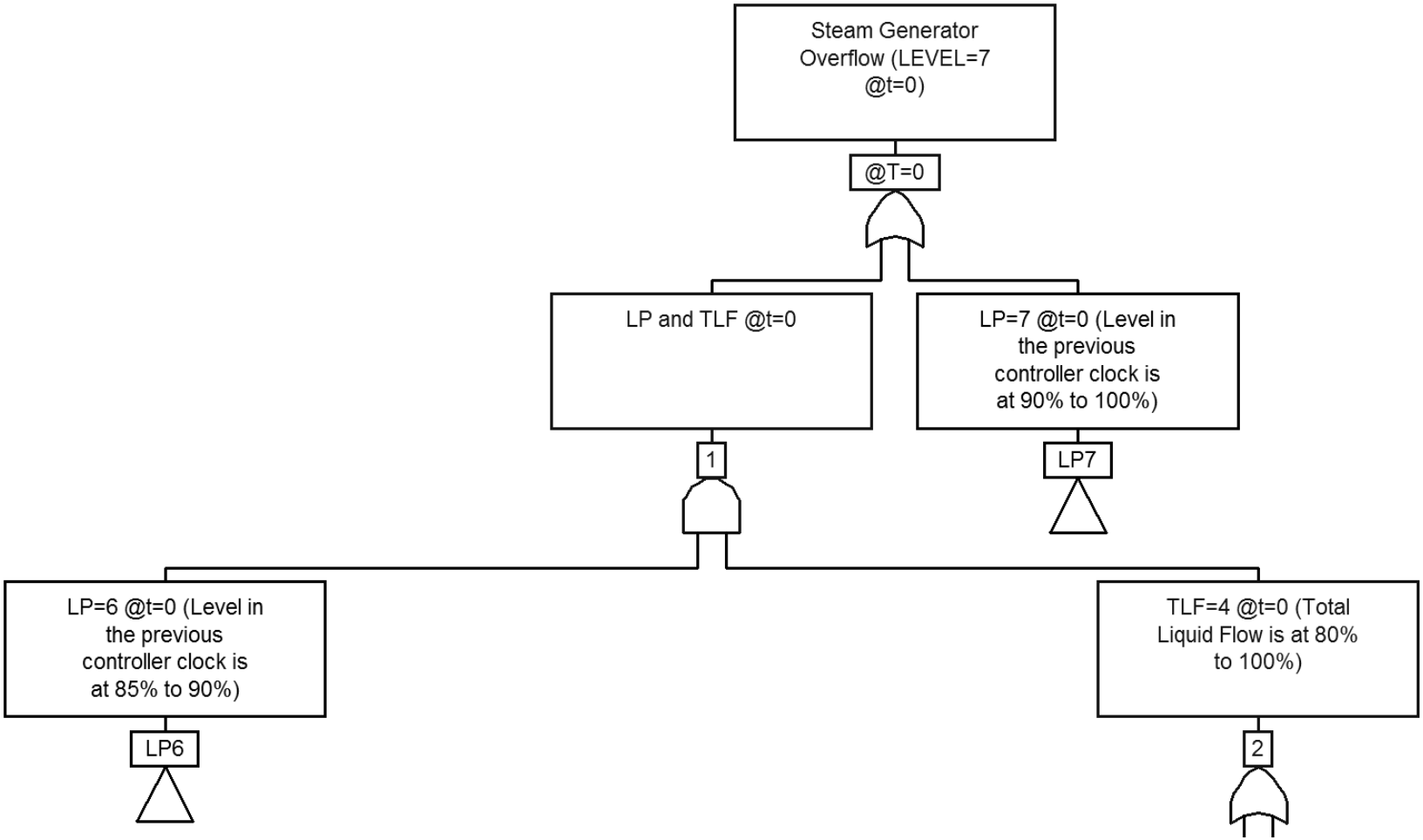
Timed-Fault Tree Generation

- Existing nuclear power plant PRAs are mostly based on conventional methods i.e., *fault tree and event tree analysis*
- *Incorporation of the Dynamic Models* into existing conventional PRAs
- A *series of static fault trees* at different time steps
- Minimal cut-sets or prime implicants are all *time-stamped*

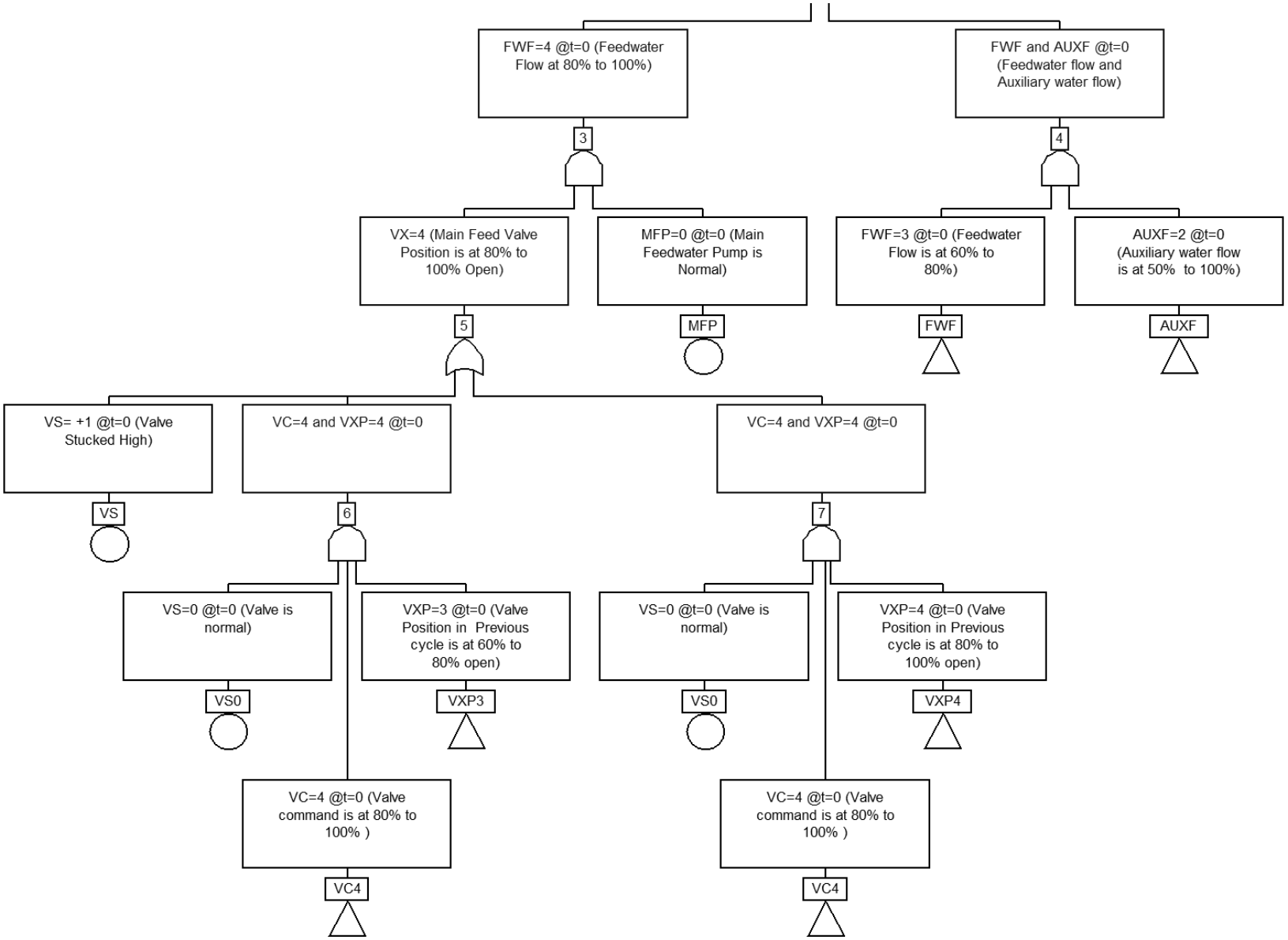
Timed-Fault Tree Construction

- Time-fault Trees are constructed by *backtracking through each of the decision tables*
- Logically and physically inconsistent branches are pruned from the tree to obtain the minimal cut-set/PIs
- Control Loop backtracking- *Redundant/occurred components pruned*
- Transition Tables *changes the time at which a particular variable occurs*

A portion of the Timed-FT

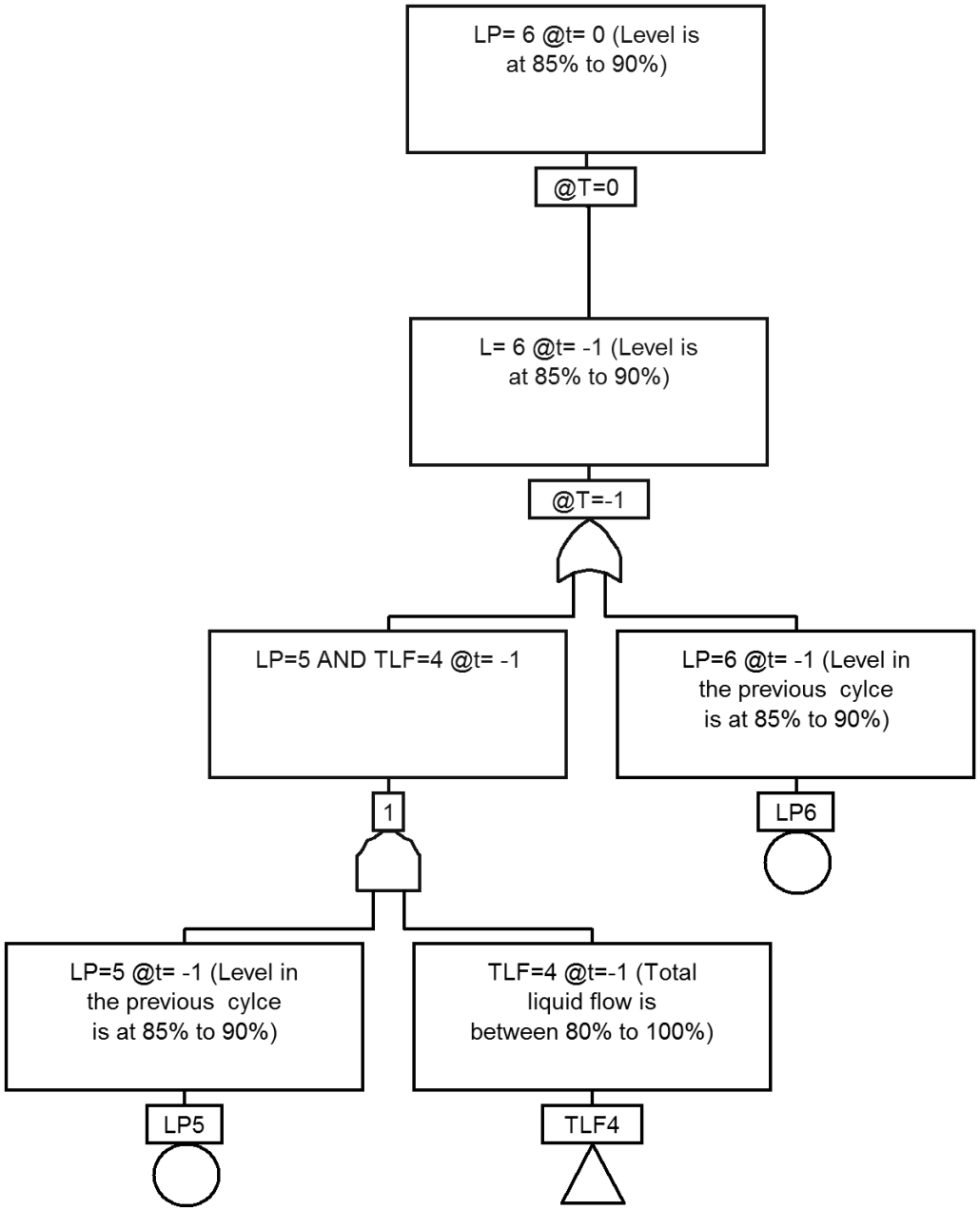


UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

26th Sept. 2017



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

26th Sept. 2017

Conclusion

- DFM provides a promising way to *adequately model and analyze digital systems* that multi-valued logic and time dependent
- Favorable approach to model dynamic systems by *explicit representation of time element* (a significant advantage over the conventional methods)
- DFM can be used as a PRA *modeling supplement for special portions of a system* that are dynamic and non-binary in behavior.

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Conclusion

- DFM Prime Implicants and minimal cut-set of the timed-fault trees agrees *(post processing)*
- *However, significant amount of time required* for post-processing of the prime implicants
- *Timed-fault trees can be incorporated* into existing PRA models to quantify the impact of a digital system

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Ongoing Research…

- System modelling utilizing *Markov/Cell-to-cell Mapping Technique*
- *Generation of Dynamic Fault Trees* from Markov/CCCMT Model
- Comparison of Fault Tree, DFM and Markov-CCMT
- *Incorporation of dynamic fault trees* into existing PRA Models *(SAPHIRE)*

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

UNIVERSITY OF ONTARIO
INSTITUTE OF TECHNOLOGY

Thank You

26th Sept. 2017