Sequential Dependency and Reliability Analysis of Embedded Systems

Yu Jiang

Tsinghua university, Beijing, China

清華大學
Tsinghua University

outline

- Motivation
- Background
  - Reliability Block Diagram, Fault Tree
  - Bayesian Network, Dynamic Bayesian Network
- Our framework
  - SDM model qualitative part structure construction
  - SDM model quantitative part structure construction
- Experiment results
- Conclusion

outline

* Motivation
* Background
* Our framework
* Experiment results
* Conclusion

motivation

Traditionally, the reliability analysis of embedded systems is realized by combinatorial methods such as Fault Tree, Reliability Block Diagram [2], Bayesian Network. Those methods are the most widely used models for reliability analysis. They are easy to use.

However, the feedbacks that make the embedded system not causal can't be represented by a FT, RBD, BN model. A straightforward extension of these models may result in a graph that has cycles, which is not acyclic.

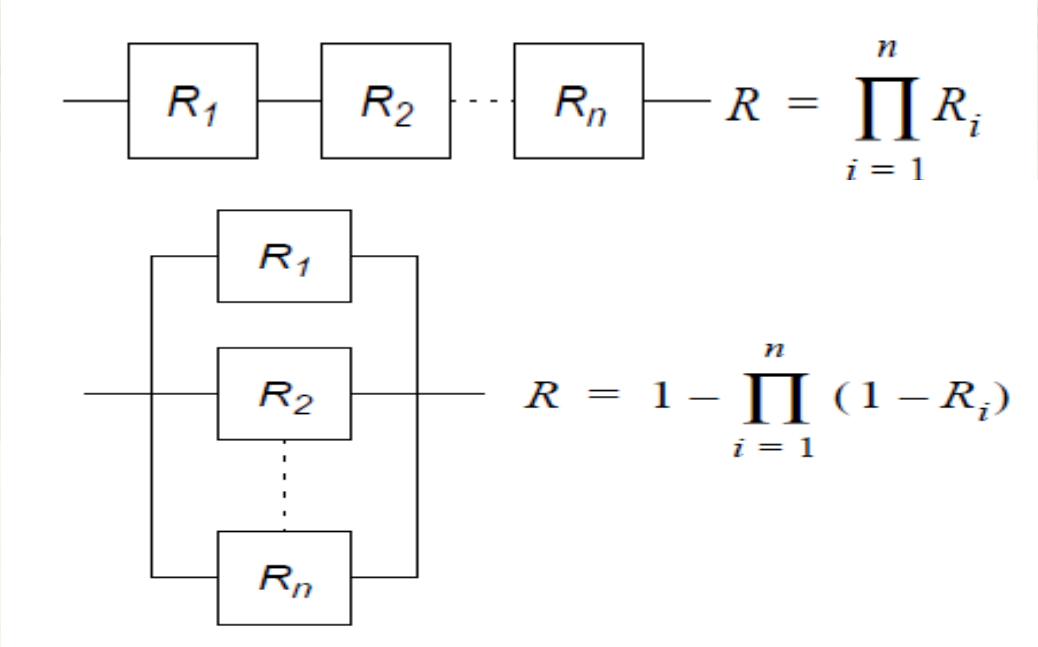
We model the feedback logic into a DBN, because DBN can handle temporal dependencies between various time slices as well as the causal dependencies at a single time slice. The proposed model is named SDM.

outline

- Motivation
- Background
  - Reliability Block Diagram, Fault Tree
  - Bayesian Network, Dynamic Bayesian Network
- Our framework
- Experiment results
- Conclusion

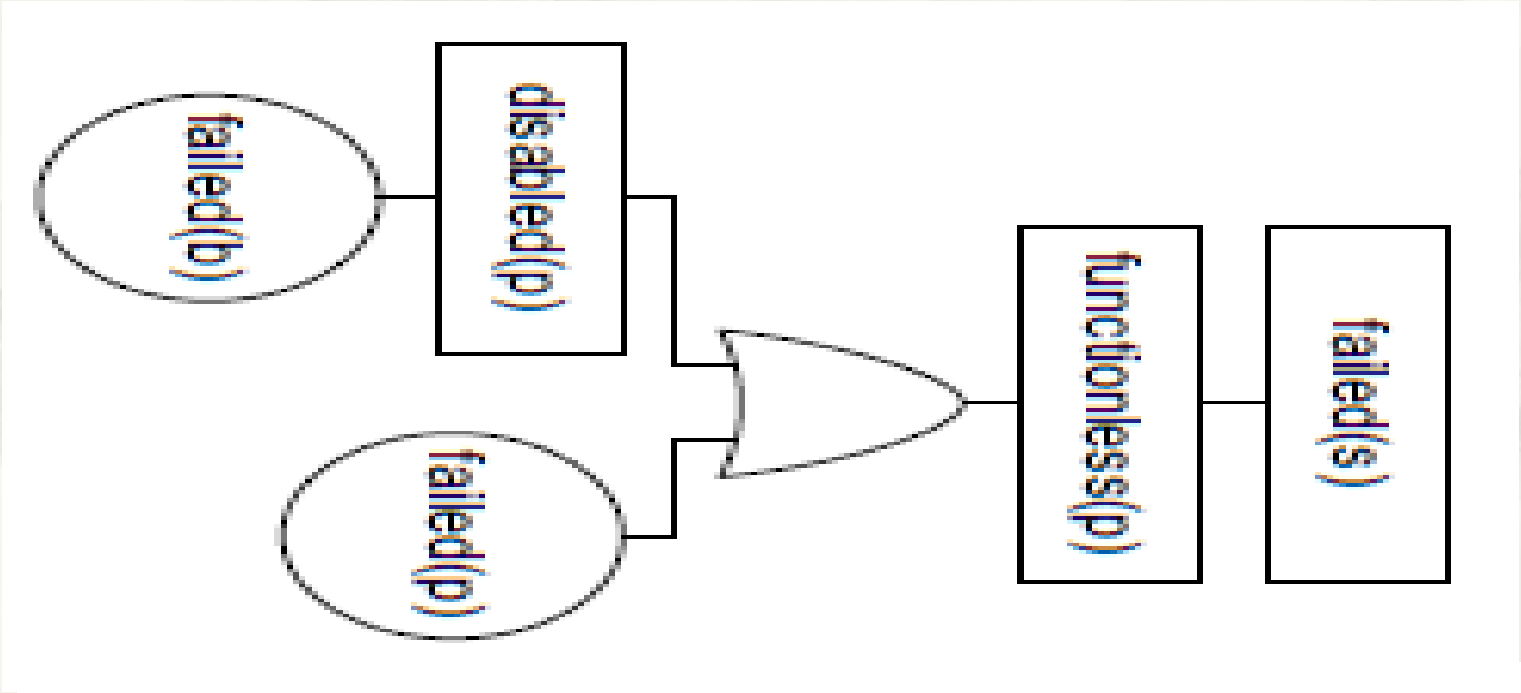
Background-Reliability Block Diagram

- reliability block diagram is a graphical depiction of the system's components and connectors which can be used to determine the overall system reliability given the reliability of its components



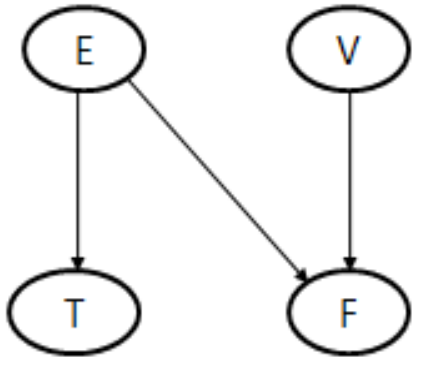
Background-Fault Tree

* FT involves specifying a top event such as the failure of the system to analyze, followed by identifying all associated events that could lead to the top event



Background-Bayesian Network

* Bayesian Network is a directed probabilistic graphical model. Each node in the graph represents a random variable, and the arc between two nodes expresses the conditional probabilistic dependency between the two random variables. The formal definition of BN is the tuple <U;E; P>.

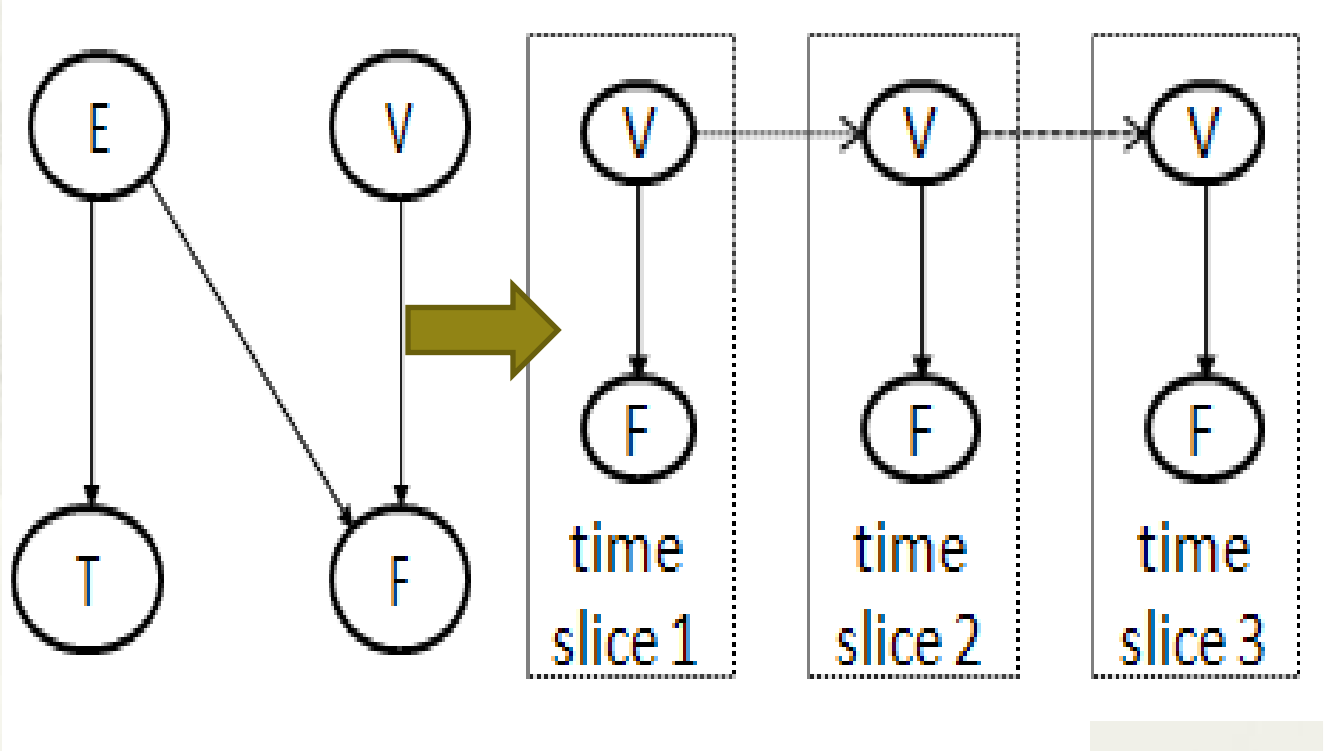


CPD FOR FIRE DISASTER(F)

$f(F\|E,V)$	$F=1$	$F=0$
$E=0,V=0$	0.1	0.9
$E=0,V=1$	0.7	0.3
$E=1,V=0$	0.6	0.4
$E=1,V=1$	0.8	0.2

Background-Dynamic Bayesian Network

* Dynamic Bayesian Network is a generalization of Bayesian Network to address stochastic processes and handle temporal effects of random variables.

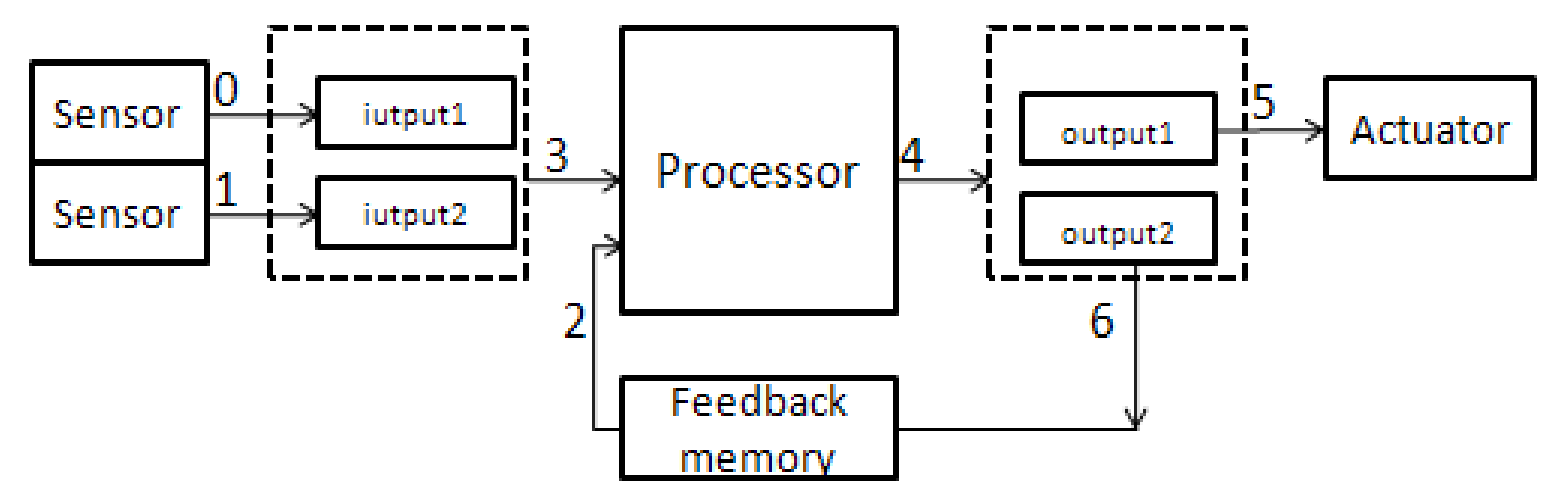


outline

- Motivation
- Background
- Our framework
  - SDM model qualitative part structure construction
  - SDM model quantitative part structure construction
- Experiment results
- Conclusion

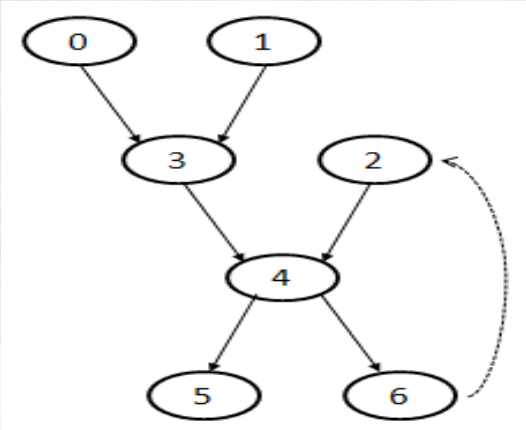
SDM-Qualitative Part Construction

* STEP 1: Determine the boundary of the sequential embedded system, identify the main components in this boundary, and describe the data signal flow through those components.
  * We can accomplish this by referring to the design document, designer, implementer and deployer of the system. We construct the model for a dedicated system.



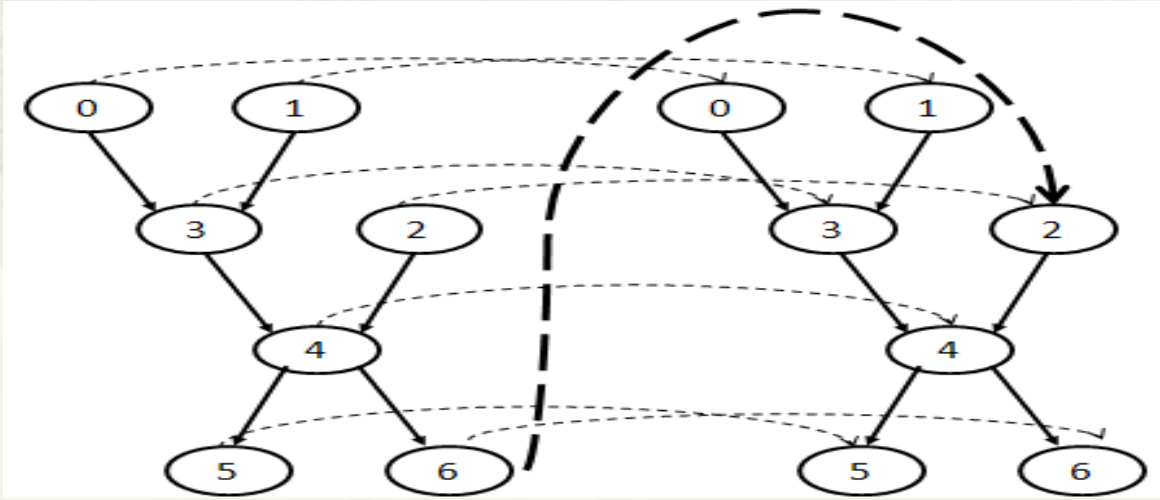
SDM-Qualitative Part Construction

* SETP 2: Construct a BN for the presented system, while ignoring the feedback. We map a node to each data signal. Edges presented in step 1 are regarded as causal or dependencies correlation. An arc is added between the nodes if the represented signals are connected by a component.
  * This can be easily finished based on the model constructed in the previous step.



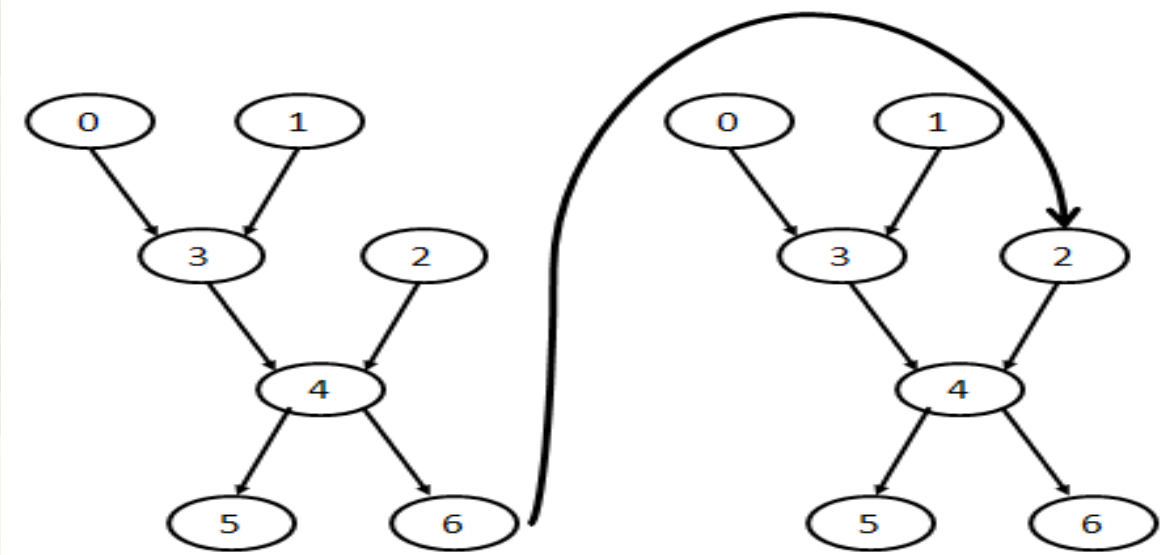
SDM-Qualitative Part Construction

- STEP 3: Unroll the constructed BN for time slices to capture the temporal dependencies caused by signal feedback and correlation between time slices.
  - This can be done by adding arcs between nodes from adjacent time slices and the feedback signals. The number of time slices is dependent on its underlying structure and different systems may need different amount of time slices to capture the temporal dependencies.



SDM-Qualitative Part Construction

* STEP 4: Modify the unrolled BN structure to get the sequential dependence model, which will be proved to be a DBN.
  * This can be done by deleting some arcs to make the unrolled BN structure minimal.



Qualitative Part Conclusion

* With these four steps, we can build a SDM to capture all those correlations among the components, especially for the feedback that makes the system not causal. Figure 6 shows the SDM for the embedded system presented in figure 3. We just unroll two time slices and the thick arcs couples the adjacent BN to handle the feedback that makes the system not causal

SDM-Quantitative Part Structure

* In a SDM, we have three kinds of nodes, the root node, the feedback node and the ordinary node.

* We need to incorporate the reliability of each component into these variables by well defined CPDs. Those CPDs for different kind of nodes and different processing structures are listed in the following tables.

Quantitative Part Structure-Root Node

TABLE I
CPD FOR THE ROOT NODE

$P(x_r^t \mid E)$	$x_r^t = 1$	$x_r^t = 0$
$E = 0$	0	1
$E = 1$	$1 - \varepsilon$	ε

Table I shows the conditional probability distribution of the root node, where E represents the environment of the system, x_r^t is the entry signal of the system and ε is the reliability of the system component that generate x_r^t

Quantitative Part Structure-Ordinary Node

TABLE II
CPD FOR THE SERIAL-PROCESSING ORDINARY NODE

$f(x_i^t \mid X_j^t)$	$x_i^t = 1$	$x_i^t = 0$
$X_j^t = \{1 \cdots 1, 1 \cdots 1\}$	$(1-\epsilon_j)^{\lvert X_j^t \rvert}$	$1-(1-\epsilon_j)^{\lvert X_j^t \rvert}$
$X_j^t = \{1 \cdots 1, 0 \cdots 0\}$	0	1

Table II shows the conditional probability distribution of the ordinary node, where X_j^t represents the parent set of x_i^t . These signals are combined in a serial manner to generate the x_i^t

清華大學
Tsinghua University

Quantitative Part Structure-Ordinary Node

TABLE III
CPD FOR THE PARALLEL-PROCESSING ORDINARY NODE

$f(x_i^t \mid X_j^t)$	$x_i^t = 1$	$x_i^t = 0$
$X_j^t = \{1 \cdots 1, 1 \cdots 1\}$	$1 - (\varepsilon_i)^{\lvert X_j^t \rvert}$	$(\varepsilon_i)^{\lvert X_j^t \rvert}$
$X_j^t = \{1 \cdots 1, 0 \cdots 0\}$	$1 - \Pi_{x_j^t = 1}(\varepsilon_i)$	$\Pi_{x_j^t = 1}(\varepsilon_i)$

Table III shows the conditional probability distribution of the ordinary node, where those parent signals are combined in parallel redundancy to generate a signal x_i^t

Quantitative Part Structure-Feedback Node

TABLE IV
CPD FOR THE FEEDBACK NODE

$f(x_i^t \mid X_j^{t-1})$	$x_i^t = 1$	$x_i^t = 0$
$X_j^{t-1} = \{1 \cdots 1, 1 \cdots 1\}$	$1 - (\varepsilon_i)^{\lvert X_j^{t-1} \rvert}$	$(\varepsilon_i)^{\lvert X_j^{t-1} \rvert}$
$X_j^{t-1} = \{1 \cdots 1, 0 \cdots 0\}$	$1 - \Pi_{x_j^t=1}(\varepsilon_i)$	$\Pi_{x_j^t=1}(\varepsilon_i)$

Table IV shows the conditional probability distribution of feedback node, where x_i^t is the feedback variable X_j^t represents parent set of x_i^t from the previous time slice.

Quantitative Part Structure Conclusion

- With those CPD tables, it is easy to incorporate the individual component reliability into the SDM model of the sequential embedded systems. What we need is to change the value of " according to the status of the system components and the stated operating environment. We can perform predictive and diagnostic inferences to study the behavior of the whole system or a single component.

outline

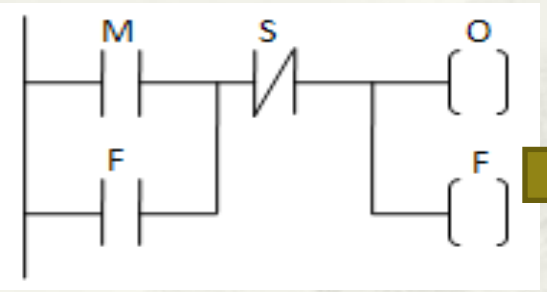
* Motivation
* Background
* Our framework
* Experiment results
* Conclusion

清華大學
Tsinghua University

Experiment-Case study

* We will illustrate our method with an example, the reliability of a sequential embedded system: PLC controller for motor. The system is used to control the motor to move forward and stop. It is consist of two sensors to sample the move instruction and the stop instruction, an I/O buffer to store the two sampled inputs, a latch memory to store the feedback input variable, a processor to process those three inputs according to the embedded ladder program shown in the figure, an I/O buffer to store the two outputs of the processer and a motor.

Experiment-Case study



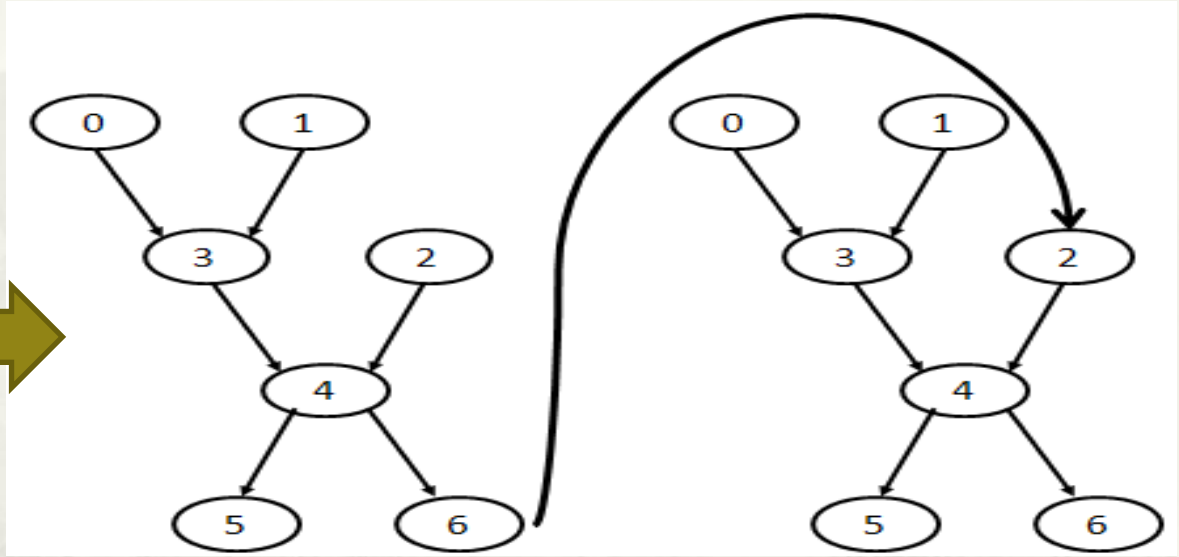


TABLE VI

STATIC FAILURE PROBABILITY OF EACH COMPONENT

component	failure probability ε
Sensor1, Sensor2	0.05
Memory	0.01
Processor	0.02
Buffer1, Buffer2	0.01

清華大學
Tsinghua University

Experiment-Case study

TABLE VI
RELIABILITY FOR THE MOTOR CONTROL SYSTEM

processor ε	BN	SDM	simulation
0.01	0.42%	0.68%	0.61%
0.02	0.67%	0.99%	0.91%
0.03	0.73%	1.09%	1.02%
0.04	0.84%	1.34%	1.25%
0.05	1.57%	2.43%	2.30%
0.06	2.31%	3.91%	3.76%
0.07	3.92%	5.01%	4.83%
0.08	4.69%	5.76%	5.52%
0.09	5.21%	6.78%	6.59%
0.10	5.67%	7.69%	7.42%

清華大學
Tsinghua University

Experiment-Complex system

TABLE VII

TABLE VIII

TABLE IX

RELIABILITY FOR THE CLARIFIER SCUM REMOVAL SYSTEM

processor ε	BN	SDM	simulation
0.01	1.57%	1.90%	1.87%
0.02	1.69%	2.31%	2.25%
0.03	2.61%	3.49%	3.42%
0.04	0.94%	4.07%	3.98%
0.05	4.59%	6.58%	6.47%
0.06	5.41%	9.10%	8.96%
0.07	7.62%	12.41%	12.10%
0.08	9.89%	14.58%	14.25%
0.09	11.31%	17.87%	17.21%
0.10	14.19%	21.11%	20.58%

outline

* Motivation
* Background
* Our framework
* Experiment results
* Conclusion

CONCLUSION

* we have constructed a sequential dependency model to handle higher order spatial and temporal dependencies among components of embedded systems, especially the dependencies caused by the feedback of component signals. We prove that the sequential dependency model is a dynamic bayesian network. Then, we model the reliability of the system as a joint distribution function of DBN over the signal nodes. The DBN model provides us a convenient way to incorporate the error probabilities of each system component to carry on predictive inference and diagnostic inference. In future, we will pay more attention to the decision order of the DBN to ensure that the reliability computation considering feedback will converge.

Thank you very much

Q/A?

清華大學
Tsinghua University