Defining futures

Formal Dependability Modeling and Analysis: A Survey

Waqar Ahmed and Osman Hasan

School of Electrical Engineering and Computer Science
National University of Sciences and Technology (NUST)
Islamabad, Pakistan

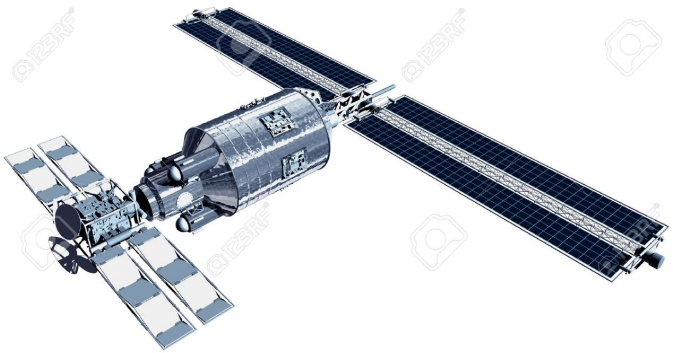
CICM 2016
Bailystock, Poland

July 27, 2016

Outline

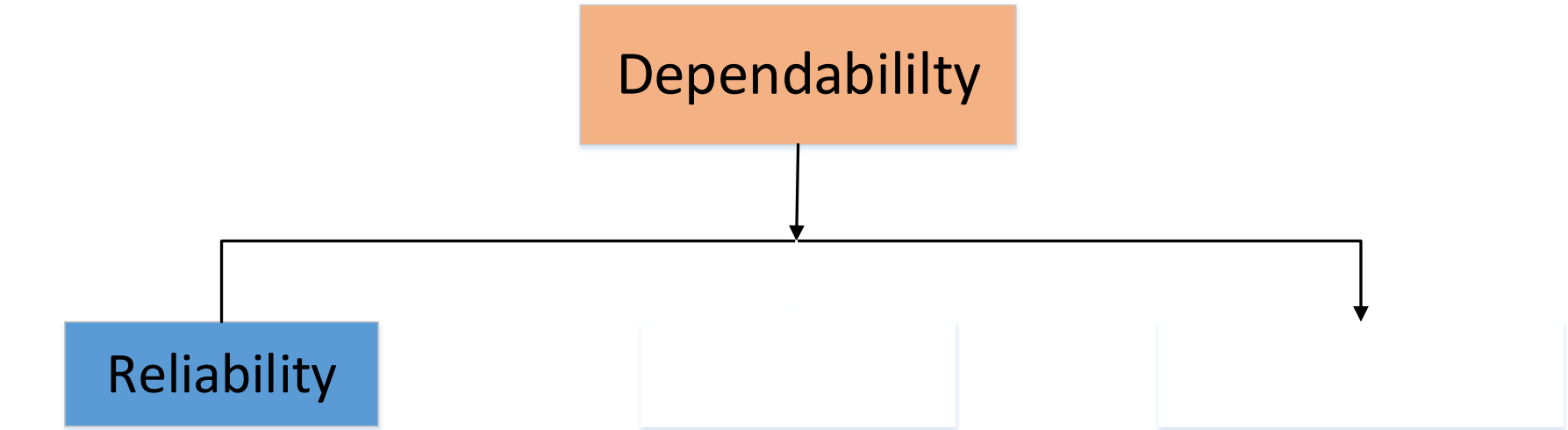
Dependability

Safety-critical Systems



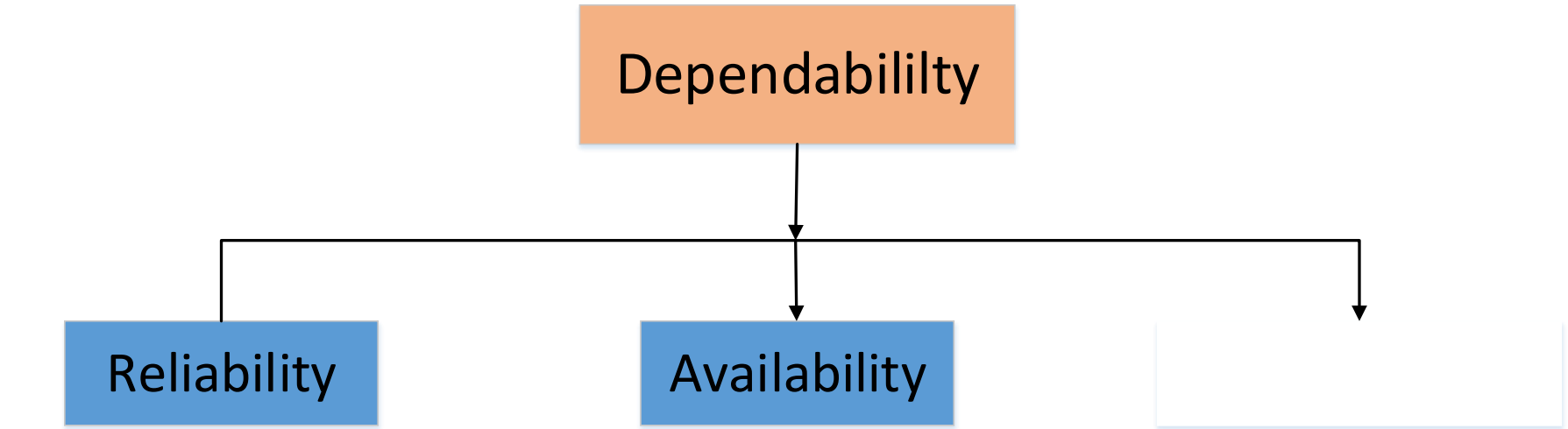
- More stringent dependability requirements
  - Main motivation for Formal Dependabiltiy Modeling and Analysis

Dependability



The ability of system to deliver services as specified within a given time

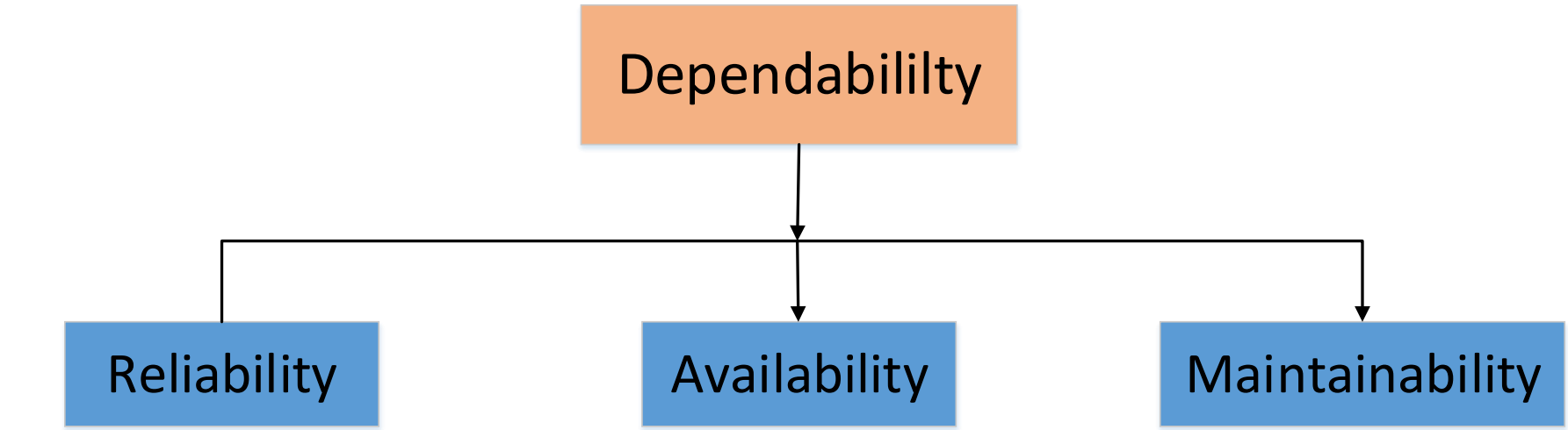
Dependability



The ability of system to deliver services as specified within a given time

The ability of system to deliver services when required

Dependability



The ability of system to deliver services as specified within a given time

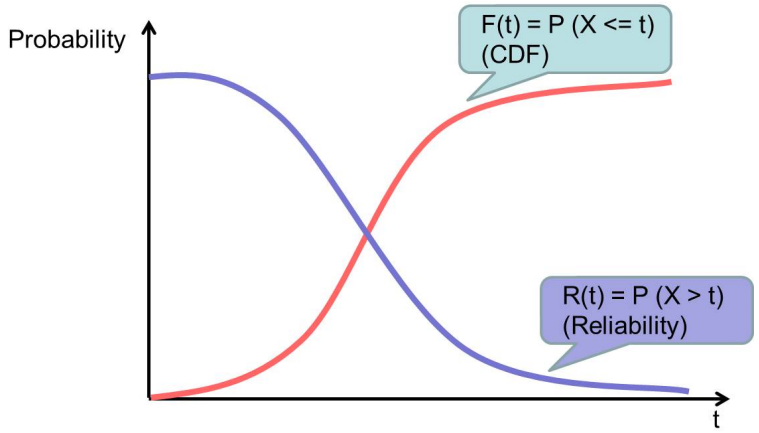
The ability of system to deliver services when required

The ability of a system to restore to operational status after a failure occurs

Formal Definitions

- Reliability $= \mathbb{P}$(no failure occurs before certain time)

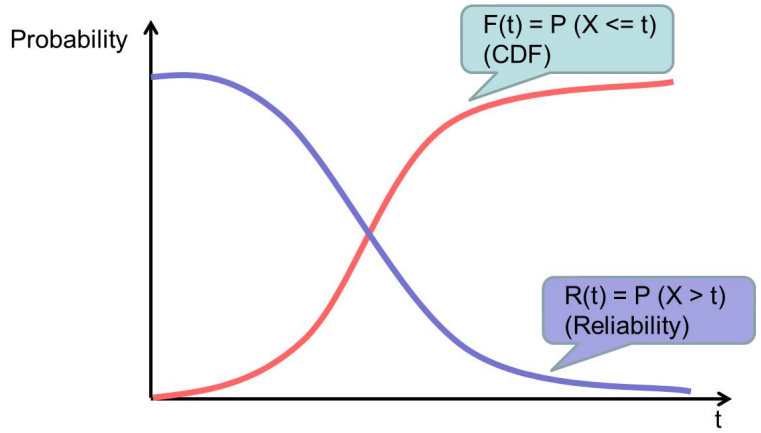
$$
\begin{aligned}
R(t) &= Pr(X > t) \\
&= 1 - Pr(X \leq t) \\
&= 1 - F_X(t)
\end{aligned}
$$



Formal Definitions

- Reliability = $\mathbb{P}$(no failure occurs before certain time)

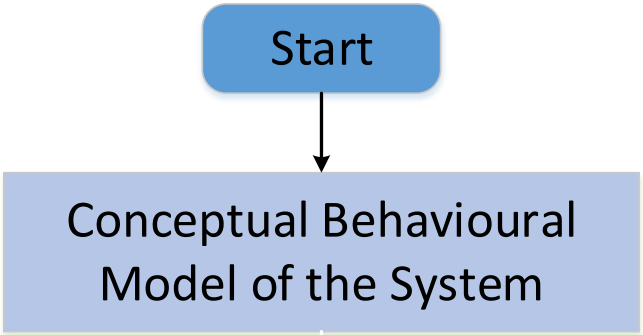
$$\begin{aligned} R(t) &= Pr(X > t) \\ &= 1 - Pr(X \leq t) \\ &= 1 - F_X(t) \end{aligned}$$



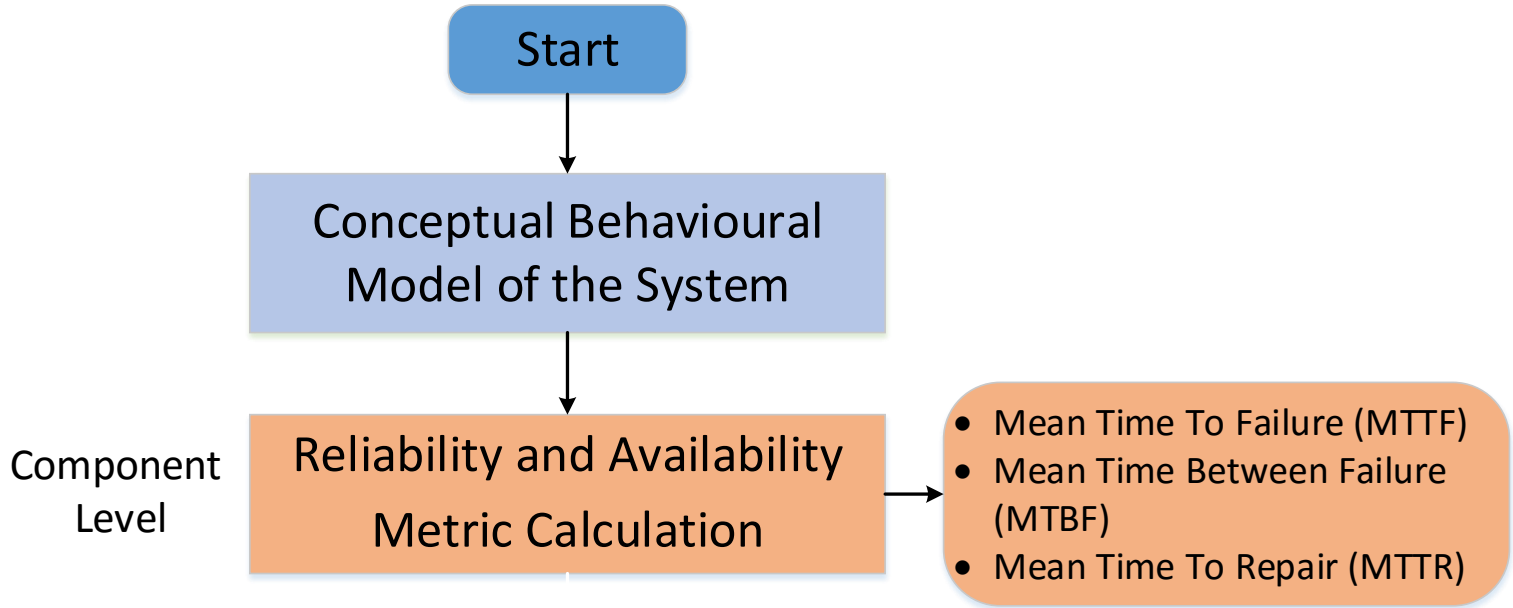
- Availability is typically derived from reliability and maintainability measures
  - A(t) = $\frac{MTBF}{MTBF + MTTR}$

    where MTBF = MTTF + MTTR
    - MTBF = Mean time between failures (Reliability Metric)
    - MTTF = Mean time to failure (Reliability Metric)
    - MTTR = Mean time to repair (Maintainability Metric)

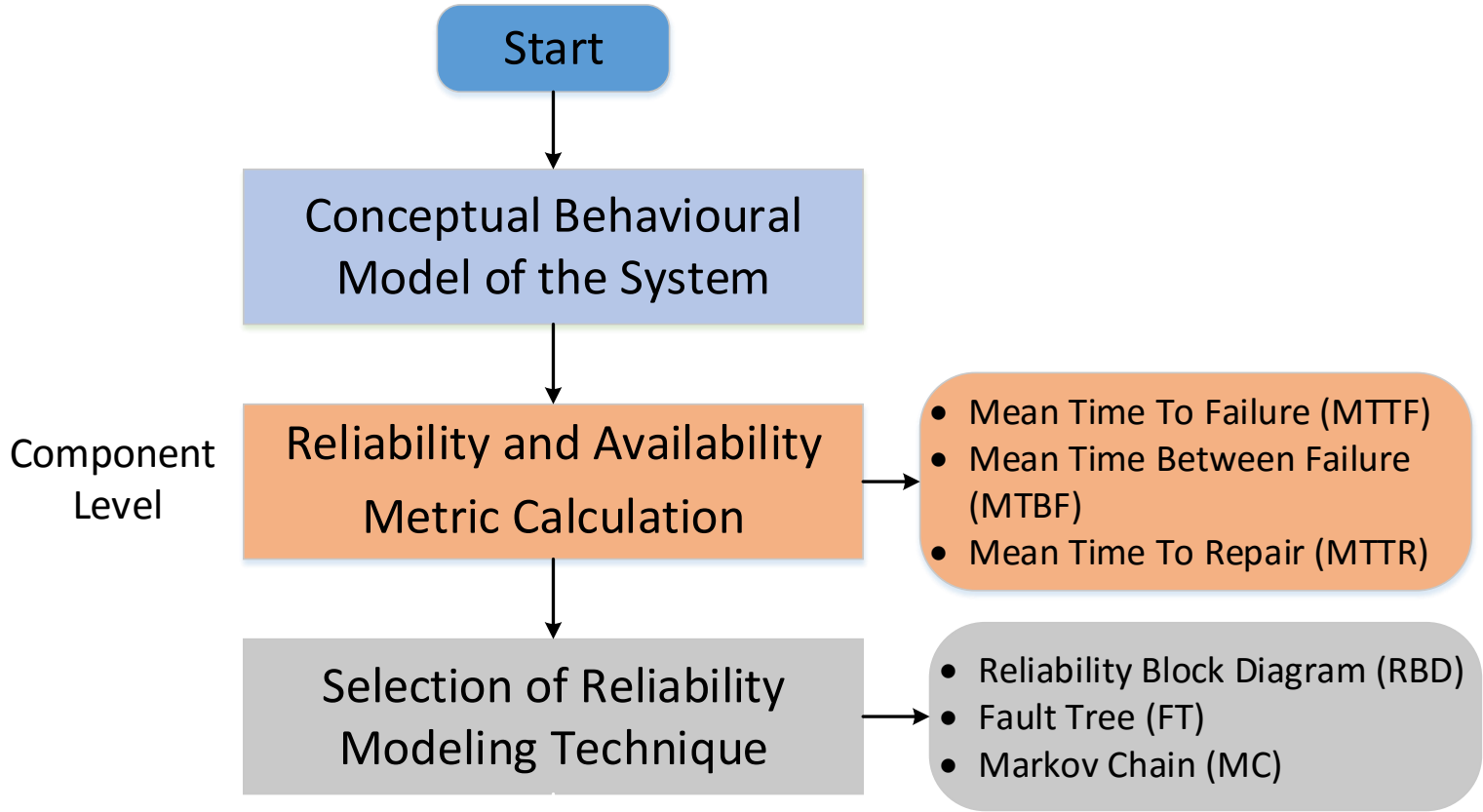
Traditional Dependability Analysis Steps



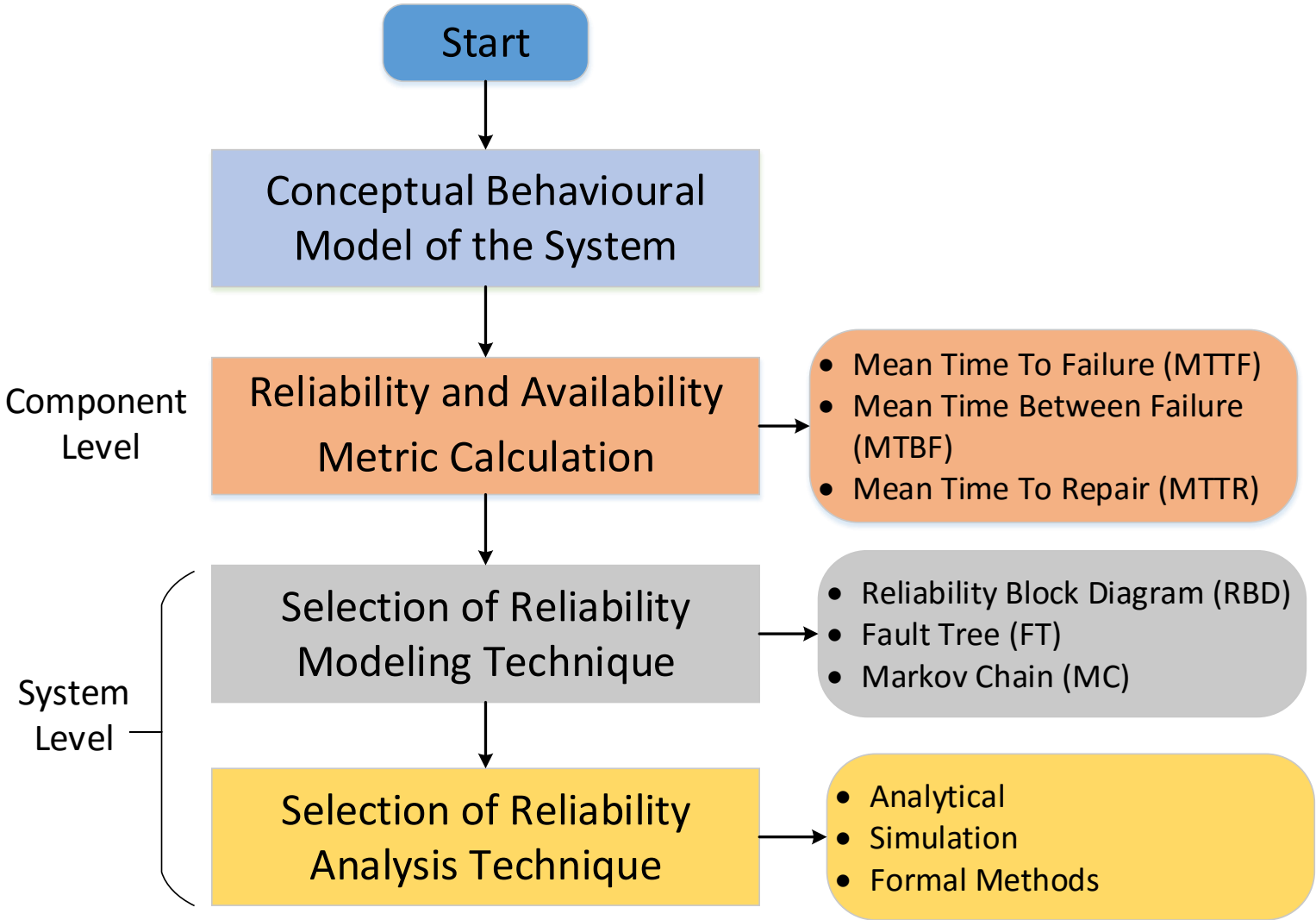
Traditional Dependability Analysis Steps



Traditional Dependability Analysis Steps



Traditional Dependability Analysis Steps



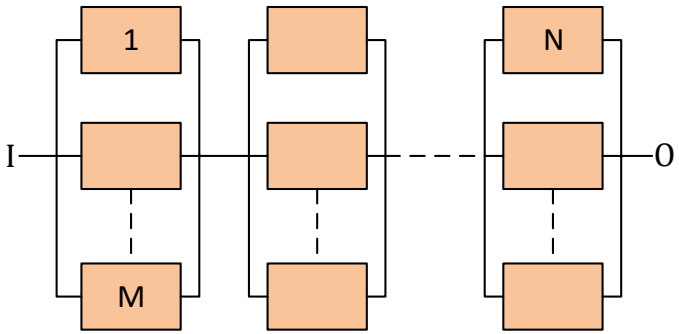
Outline

Dependability Modeling Techniques

- Some widely used modeling techniques are:
  - Reliability Block Diagram
  - Fault Tree
  - Markov Chain

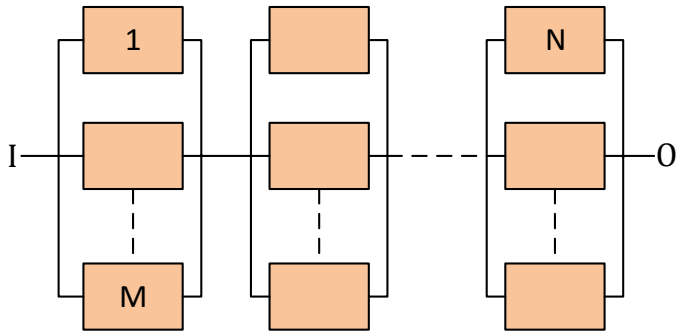
Reliability Block Diagrams

- Model the failure relationship of system components as a diagram of sub-blocks and connectors (RBD)
- Judge the failure characteristics of the overall system based on the failure rates of sub-blocks



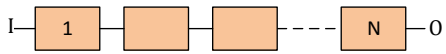
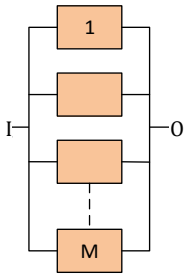
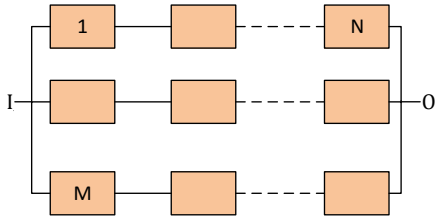
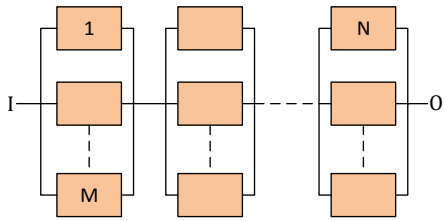
Reliability Block Diagrams

- Model the failure relationship of system components as a diagram of sub-blocks and connectors (RBD)
- Judge the failure characteristics of the overall system based on the failure rates of sub-blocks

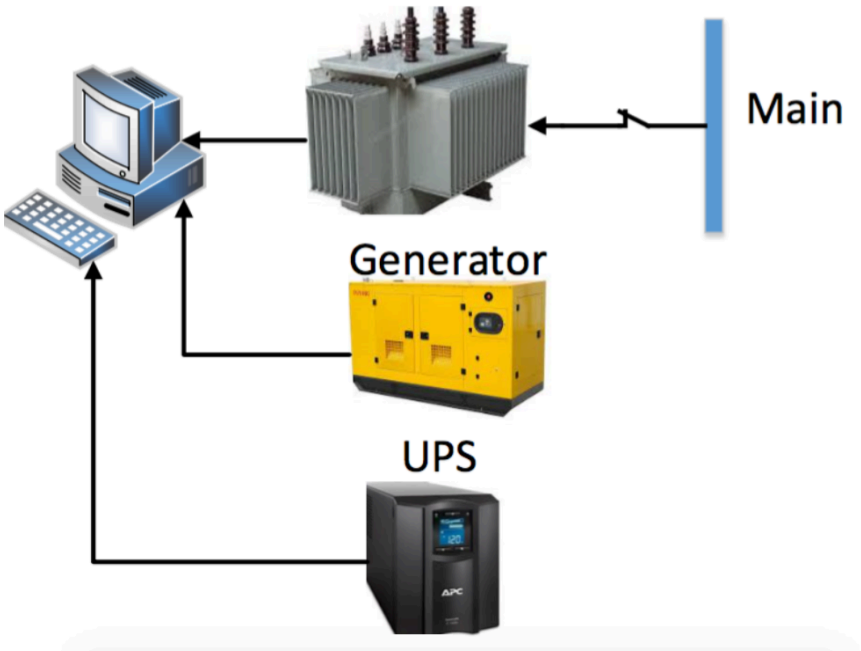


- The overall system failure happens if all the paths for successful execution fail
  - Add more parallelism to meet the dependability goals

Types of RBD

RBDs	Mathematical Expressions
	$R_{series}(t) = Pr(\bigcap_{i=1}^{N} E_i(t)) = \prod_{i=1}^{N} R_i(t)$
	$R_{parallel}(t) = Pr(\bigcup_{i=1}^{M} E_i) = 1 - \prod_{i=1}^{M}(1 - R_i(t))$
	$R_{parallel-series}(t) = Pr(\bigcup_{i=1}^{M}\bigcap_{j=1}^{N} E_{ij}(t)) = 1 - \prod_{i=1}^{M}(1 - \prod_{j=1}^{N}(R_{ij}(t)))$
	$R_{series-parallel}(t) = Pr(\bigcap_{i=1}^{N}\bigcup_{j=1}^{M} E_{ij}(t)) = \prod_{i=1}^{N}(1 - \prod_{j=1}^{M}(1 - R_{ij}(t)))$

Example: Power Supply System

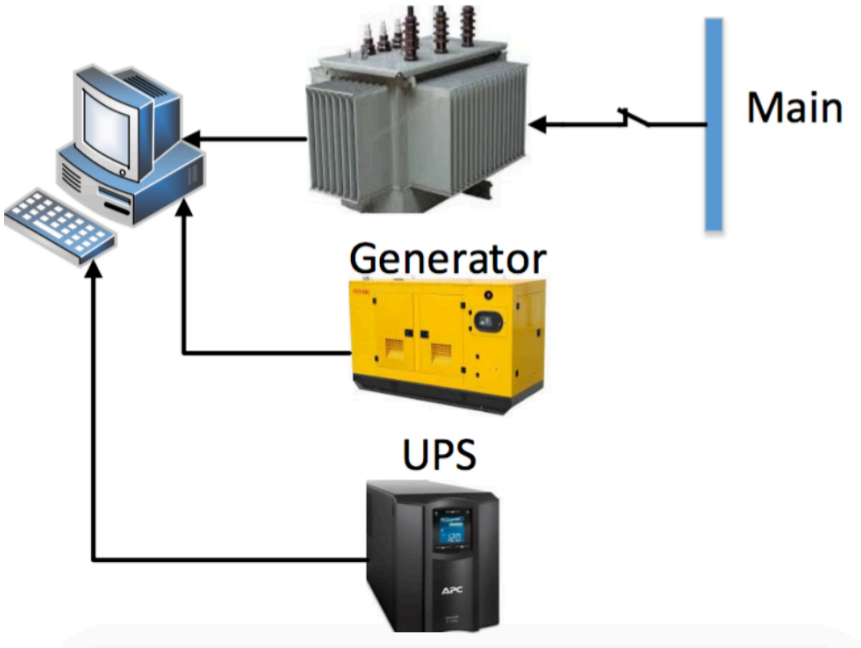


- Waqar requires continuous supply of power for his Lab PC
  - The UPS can support the load during a switch from the main supply to the generator
- Wants to determine the reliability of power supply system

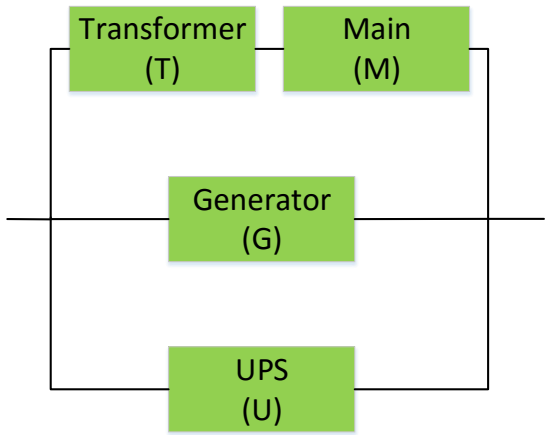
Example: Power Supply System

Step 1

Construct an RBD Model



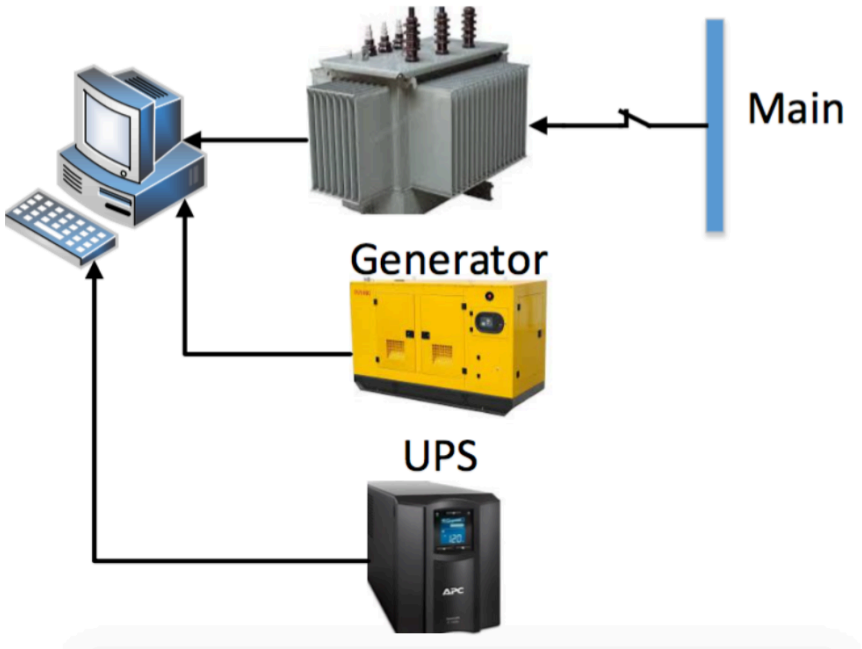
Power Supply RBD



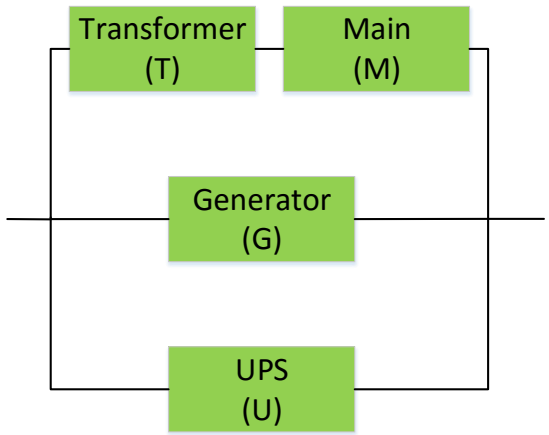
Example: Power Supply System

Step 1

Construct an RBD Model



Power Supply RBD



$$\texttt{pow\_sys\_rbd} = (\texttt{M} \cap \texttt{T}) \cup \texttt{G} \cup \texttt{U}$$

Example: Power Supply System

Step 2

Identify the RBD type

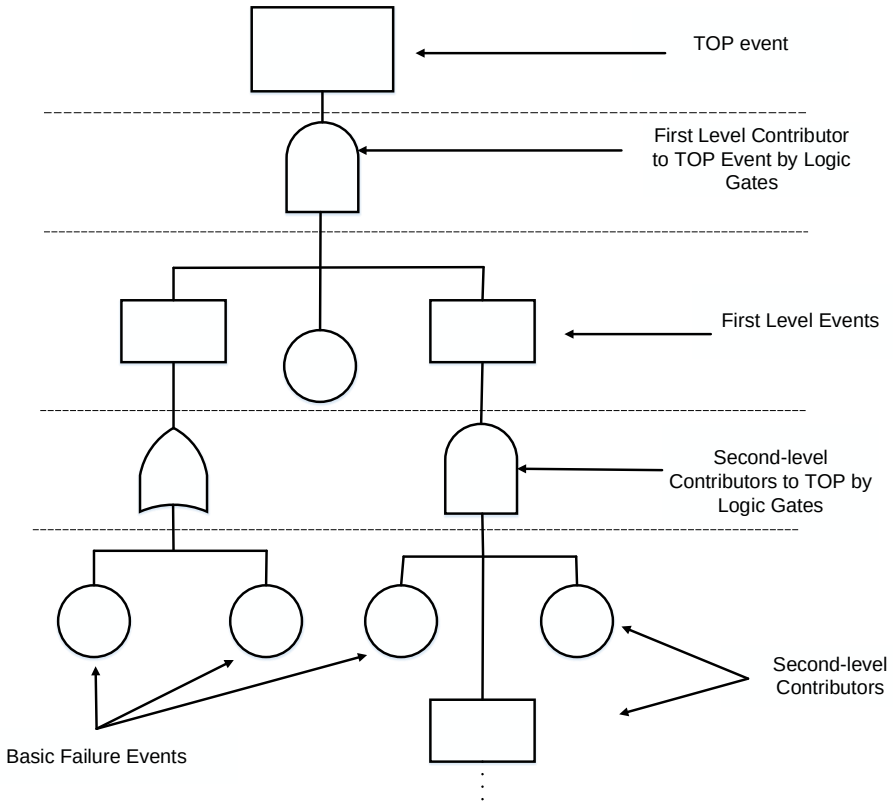
Step 3

Use the corresponding mathematical expression to evaluate the overall reliability based on the sub-components reliability

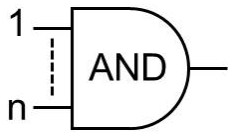
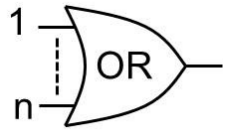
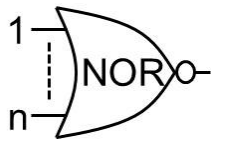
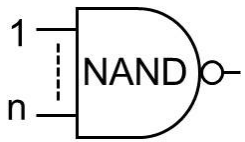
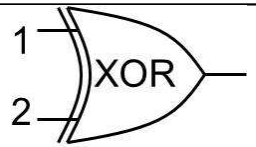
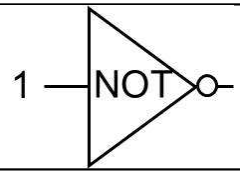
$$\mathbb{P}((\mathtt{M} \cap \mathtt{T}) \cup \mathtt{G} \cup \mathtt{U}) = 1 - (1 - \mathbb{P}(\mathtt{M}) * \mathbb{P}(\mathtt{T})) * (1 - \mathbb{P}(\mathtt{G})) * (1 - \mathbb{P}(\mathtt{U}))$$

Fault Tree

- A graphical method used to identify potential causes of system failure
- A fault tree is constructed having
  - Events: describing the failure of system components
  - Logic Gates: representing logical relationship between events
    - AND, OR, NOR, NAND, NOR etc.

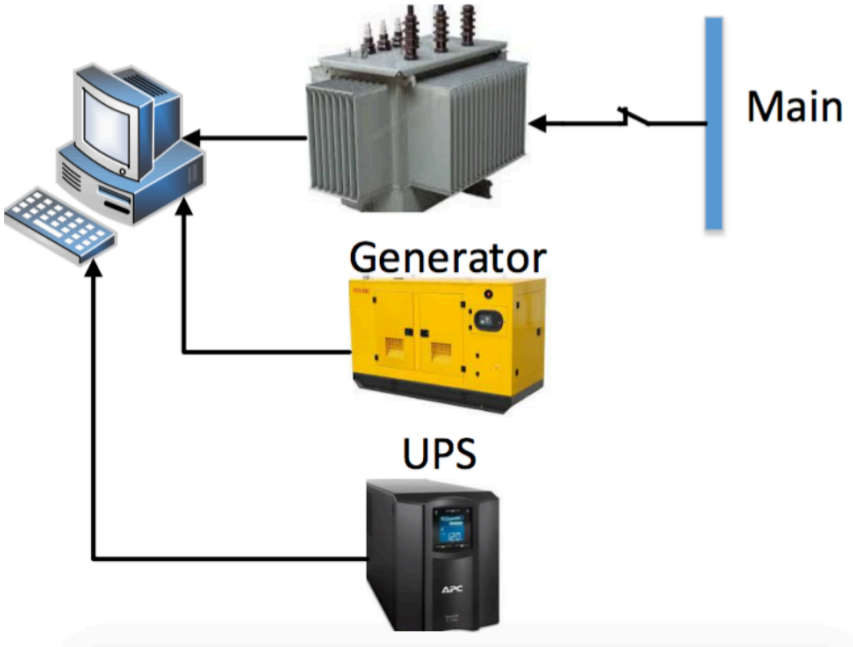


Types of FT Gates

FT Gates	Failure Probability Expressions
	$F(t) = Pr(\bigcap_{i=2}^{N} A_i(t)) = \prod_{i=2}^{N} F_i(t)$
	$F(t) = Pr(\bigcup_{i=2}^{N} A_i(t)) = 1 - \prod_{i=2}^{N}(1 - F_i(t))$
	$F(t) = 1 - F_{OR}(t) = \prod_{i=2}^{N}(1 - F_i(t))$
	$F(t) = Pr(\bigcap_{i=2}^{k} \overline{A}_i(t) \cap \bigcap_{j=k}^{N} A_i(t)) = \prod_{i=2}^{k}(1 - F_i(t)) * \prod_{j=k}^{N}(F_j(t))$
	$F(t) = Pr(\bar{A}(t)B(t) \cup A(t)\bar{B}(t))$ $= F_A(t)(1 - F_B(t)) + F_B(t)(1 - F_A(t))$
	$F(t) = Pr(\bar{A}(t)) = (1 - F_A(t))$

Example: Power Supply System

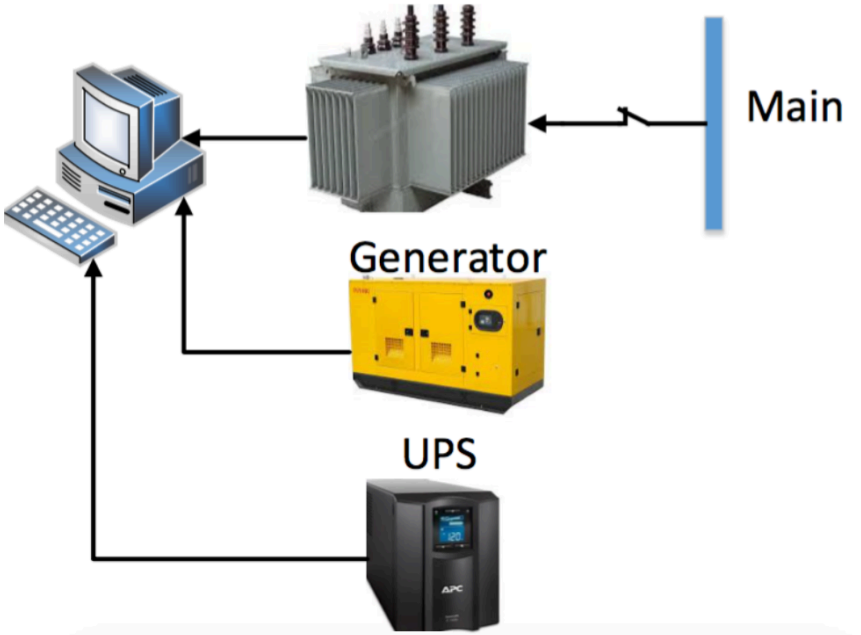
- Determine the overall failure probability?

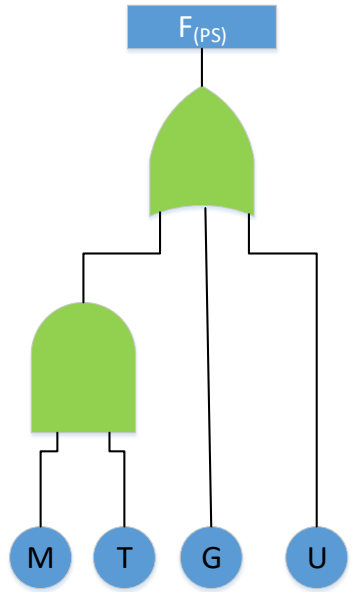


Fault Tree Analysis

Step 1

Construct a FT and represent Top Event in terms of basic events

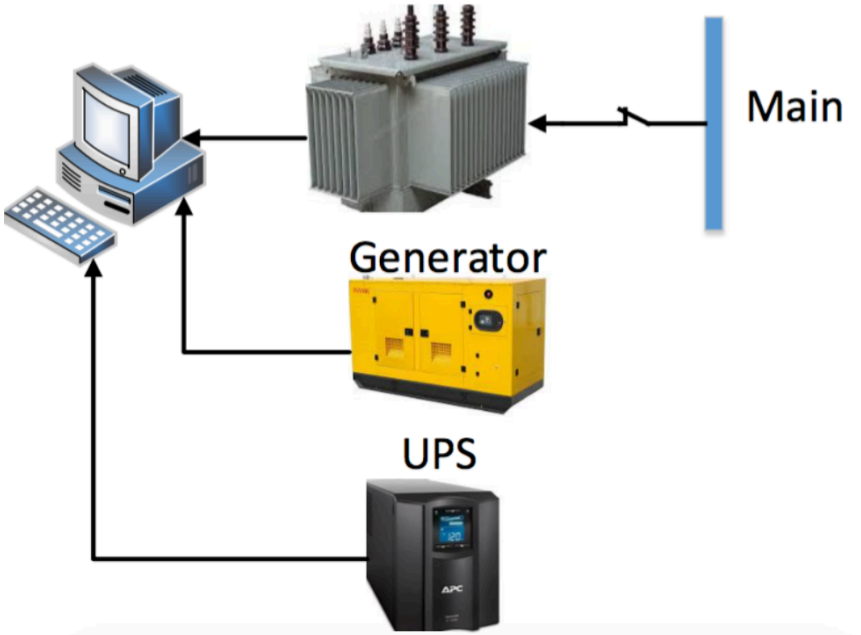


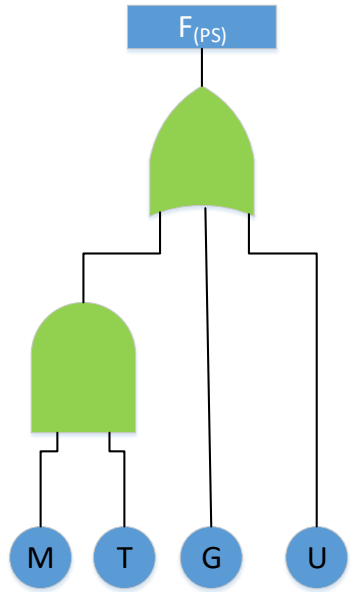


Fault Tree Analysis

Step 1

Construct a FT and represent Top Event in terms of basic events





$$pow\_sys\_fail = (M \cup T) \cap G \cap U$$

Fault Tree Analysis

Step 2

Evaluate probability of failure using the Probabilistic Inclusion-Exclusion principle

$$\mathbb{P}(\bigcup_{i=1}^{n} A_i) = \sum_{J \neq \emptyset, J \subseteq \{1,2,\ldots,n\}} (-1)^{|J|-1} \mathbb{P}(\bigcap_{j \in J} A_j)$$

$$\begin{aligned}\mathbb{P}(pow\_sys\_fail) &= \mathbb{P}((M \cup T) \cap G \cap U) \\ &= \mathbb{P}(M \cap G \cap U) + \mathbb{P}(T \cap G \cap U) - \mathbb{P}(M \cap T \cap G \cap U)\end{aligned}$$

Step 3

Using Mutual Independence property

$$\mathbb{P}(pow\_sys\_fail) = \mathbb{P}(M) * \mathbb{P}(G) * \mathbb{P}(U) + \mathbb{P}(T) * \mathbb{P}(G) * \mathbb{P}(U) - \mathbb{P}(M) * \mathbb{P}(T) * \mathbb{P}(G) * \mathbb{P}(U)$$

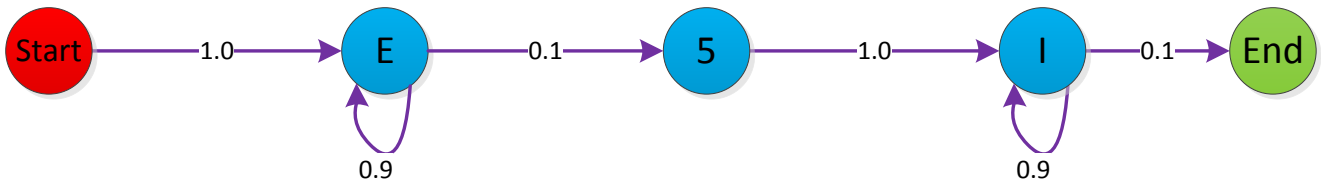
Markov Chain

- Stochastic Process

- Markov Property

Markov Chain

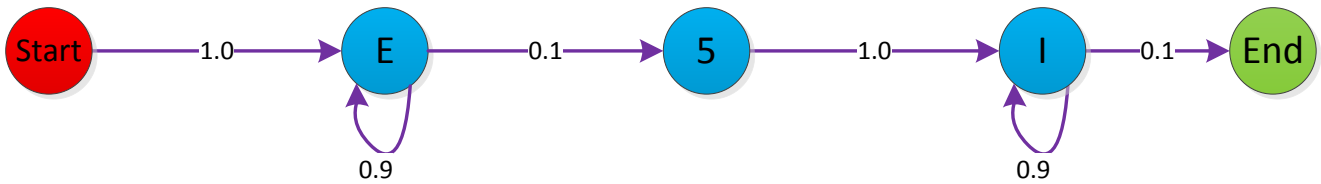
- Stochastic Process
  - A sequence of states
  - Determining the next state is random



- Markov Property

Markov Chain

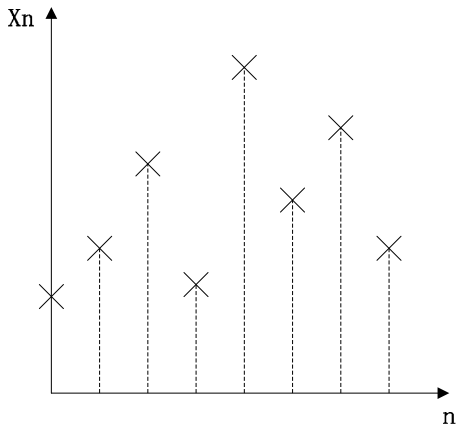
- Stochastic Process
  - A sequence of states
  - Determining the next state is random



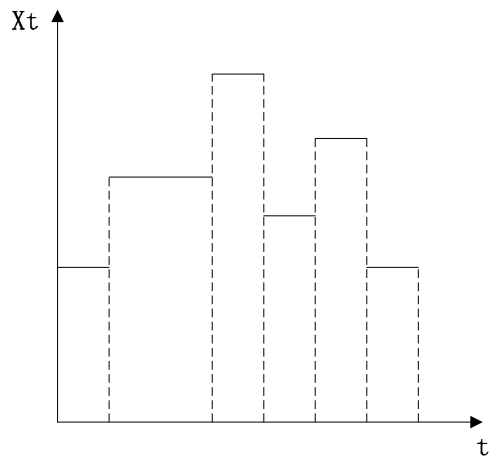
- Markov Property
  - The probability of the next state is only dependent on the current state

$$\mathcal{P}r\{X_{t_{n+1}} = f_{n+1} | X_{t_n} = f_n, \ldots, X_{t_0} = f_0\} = \mathcal{P}r\{X_{t_{n+1}} = f_{n+1} | X_{t_n} = f_n\}$$

Markov Chains - Types



Discrete-time Markov Chain



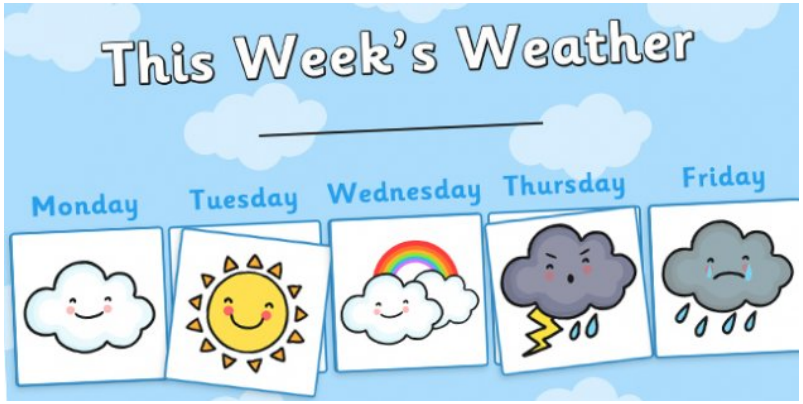
Continuous-time Markov Chain

Markov Chain - Example

- Weather Prediction Problem

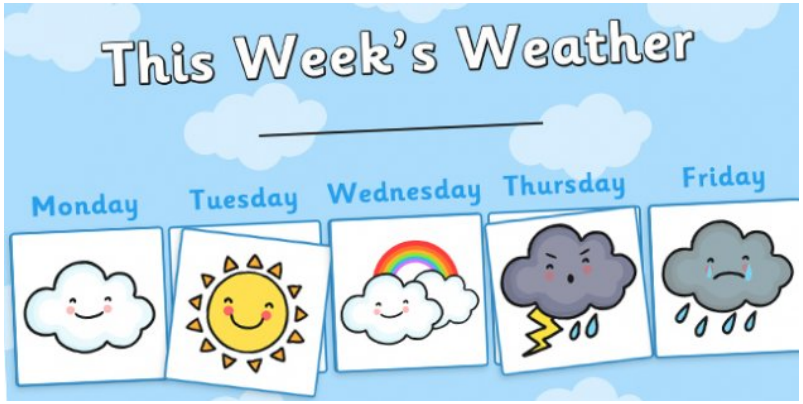
Markov Chain - Example

- Weather Prediction Problem
  - Waqar records the weather conditions (sunny or rainy/snowy) daily



Markov Chain - Example

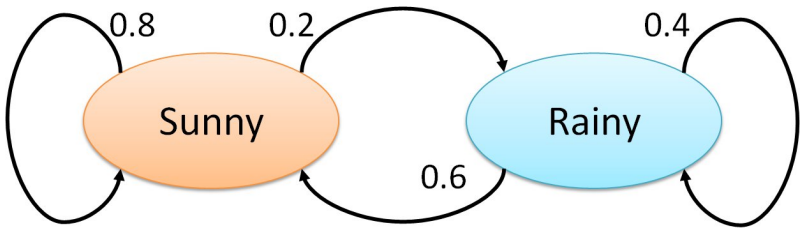
- Weather Prediction Problem
  - Waqar records the weather conditions (sunny or rainy/snowy) daily



  - Based on this collected data he wants to obtain the probability of a specific weather pattern

Markov Chain - Example

- Solution: Discrete Time Markov Chains
  - Set of States = {Sunny, Rainy}
  - State Transition Probabilities can be obtained from the observed data
    - Example: P{"Tomorrow is sunny" given that "Today is sunny"}



Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain

Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Paths between input and output	✓		✓

Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Paths between input and output	✓		✓
Failure Paths between input and output		✓	✓

Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Paths between input and output	✓		✓
Failure Paths between input and output		✓	✓
Combinatorial Problems (Effect of sub-components on the failure of the whole system)	✓	✓	✓

Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Paths between input and output	✓		✓
Failure Paths between input and output		✓	✓
Combinatorial Problems (Effect of sub-components on the failure of the whole system)	✓	✓	✓
Non-combinatorial Problems (System is either inactive, failure or in standby state)			✓

Comparison between Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Paths between input and output	✓		✓
Failure Paths between input and output		✓	✓
Combinatorial Problems (Effect of sub-components on the failure of the whole system)	✓	✓	✓
Non-combinatorial Problems (System is either inactive, failure or in standby state)			✓
Large and Complex Systems	✓	✓	

Outline

Formal Dependability Analysis Techniques

Dependability models have been analyzed extensively using the following formal techniques:

- Petri Nets
- Model Checking
- Higher-order-Logic Theorem Proving

Petri Nets

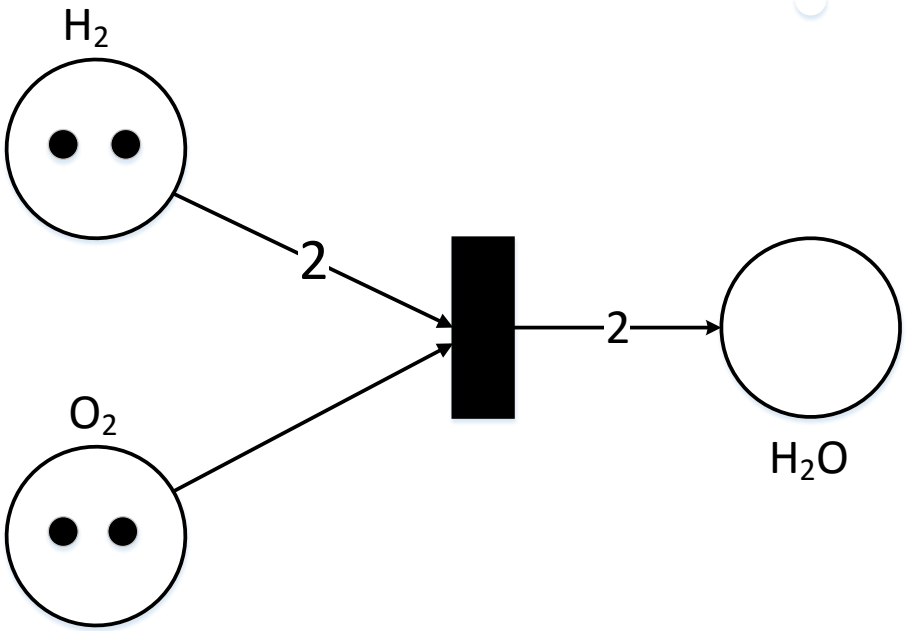
- A Petri Net is a bipartite graph consisiting of:

Places Transitions Tokens

- Transitions consume tokens from the input places and produce tokens in the output places

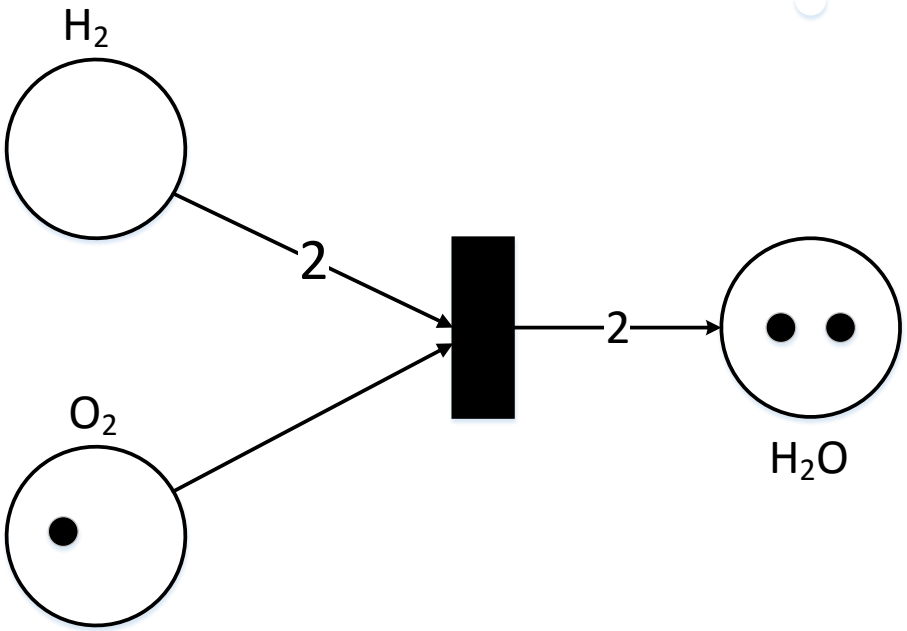
Example: Chemical Reaction

$$2H_2 + O_2 \Rightarrow 2H_2O$$



Example: Chemical Reaction

$$2H_2 + O_2 \Rightarrow 2H_2O$$



Dependability Analysis using Petri Nets:

- Colored PN (CPN) and Stochastic PN (SPN) have been extensively used for dependability analysis

Dependability Analysis using Petri Nets:

- Colored PN (CPN) and Stochastic PN (SPN) have been extensively used for dependability analysis

- Analyzing RBDs and FTs with Petri Nets
  - Broadband Integrated Service Network (Balakrishnan et al. RESS-1996)
  - Internet voting System (Omidi et al. Computer & Comm. Eng., 2012)
  - High-speed Trains (Lijie et al. RESS-2012)
  - Logistic Supply Chain (Li et al. IJUNESST-2014)

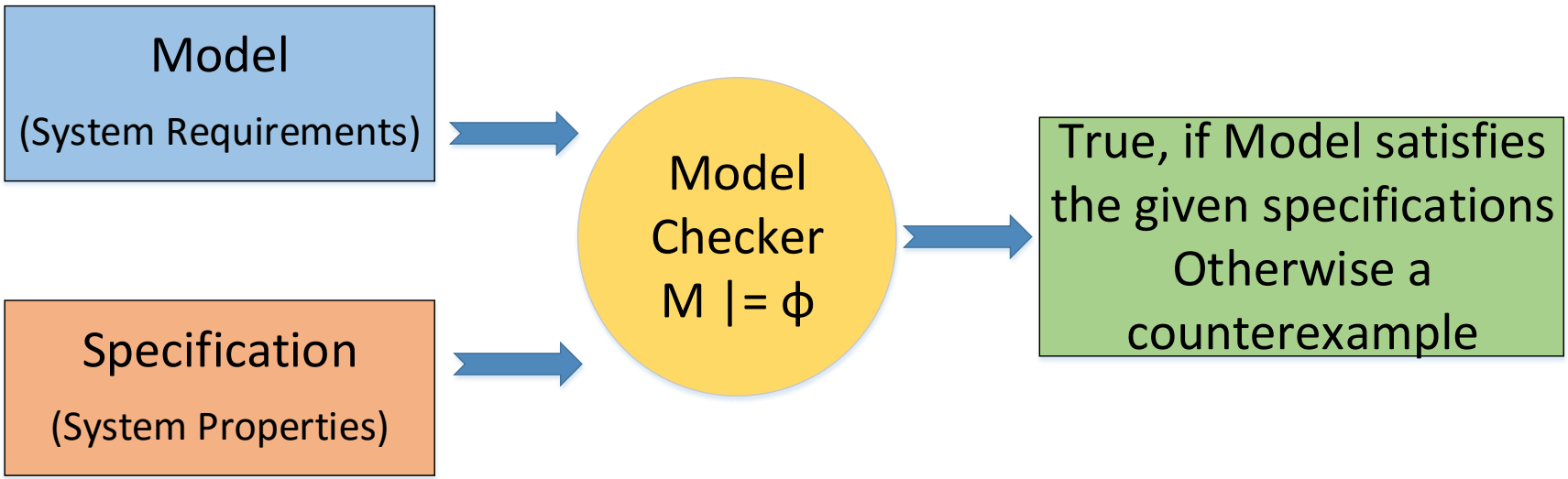
Dependability Analysis using Petri Nets:

- Colored PN (CPN) and Stochastic PN (SPN) have been extensively used for dependability analysis

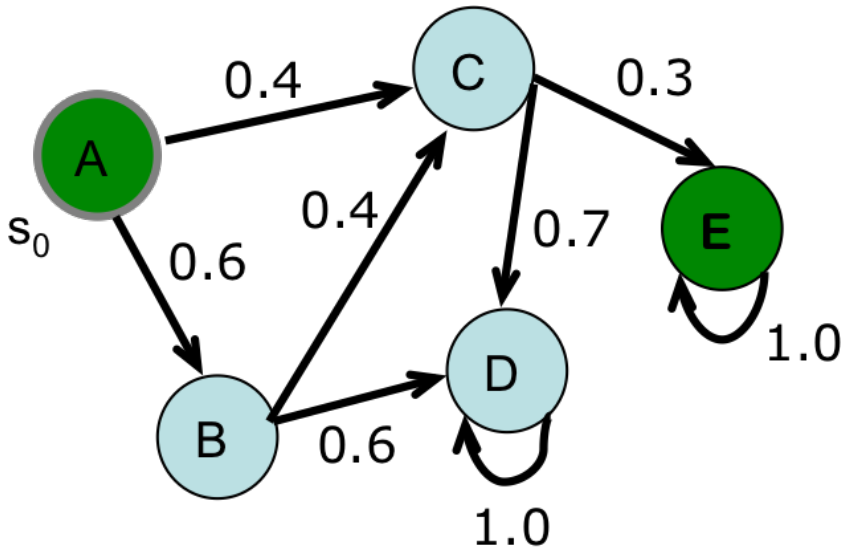
- Analyzing RBDs and FTs with Petri Nets
  - Broadband Integrated Service Network (Balakrishnan et al. RESS-1996)
  - Internet voting System (Omidi et al. Computer & Comm. Eng., 2012)
  - High-speed Trains (Lijie et al. RESS-2012)
  - Logistic Supply Chain (Li et al. IJUNESST-2014)

- Analyzing Markov chains with PNs
  - Client Server Queuing system (Ibe et al. TPDS-1993)
  - Fibre Distributed Data Interface (FDDI) (Christodoulou et al. ETFA-1994)
  - Low Earth Orbit (LEO) satellite (Zeng et al. JMLC-2011)

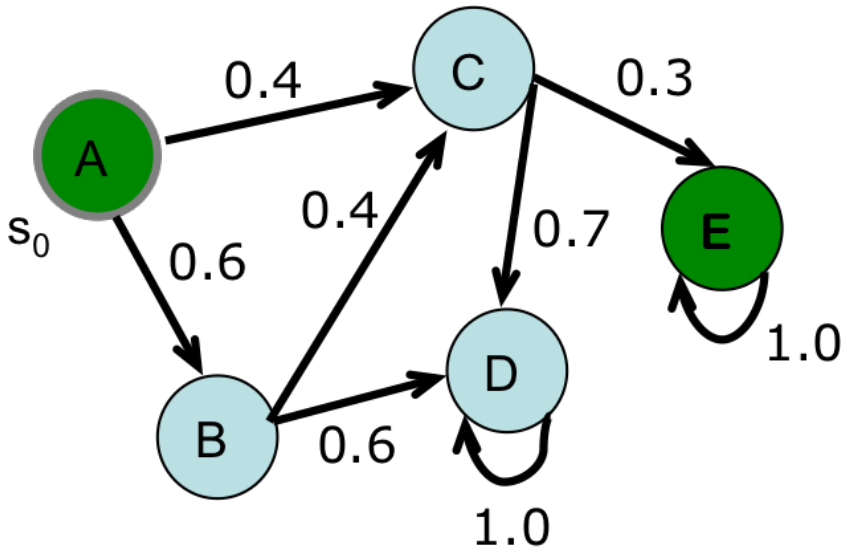
Model Checking



Probabilistic Model Checking - Example

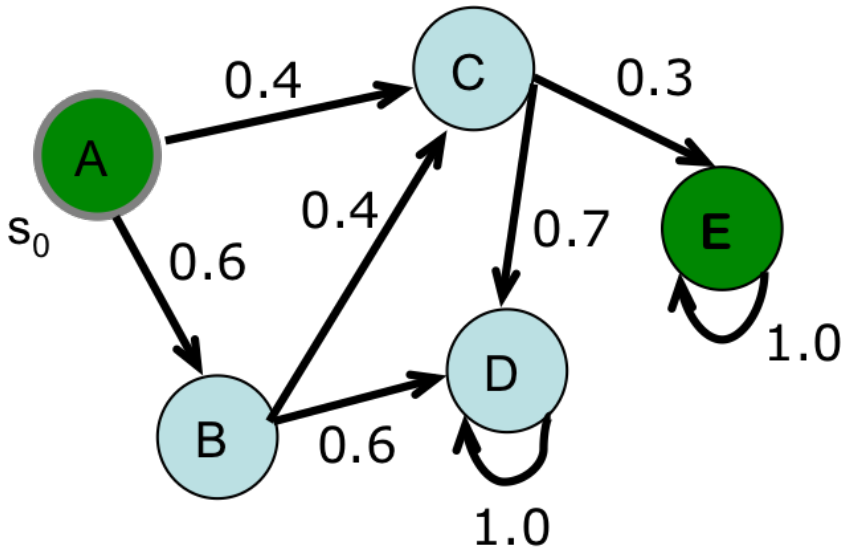


Probabilistic Model Checking - Example



- Probability of reaching State E from the State A:
  $0.4x0.3 + 0.6x0.4x0.3 = 0.192$

Probabilistic Model Checking - Example



- Probability of reaching State E from the State A:
  $0.4x0.3 + 0.6x0.4x0.3 = 0.192$
- Probabilities associated with the validity of Temporal logic properties can be verified

Dependability Analysis using Model Checking

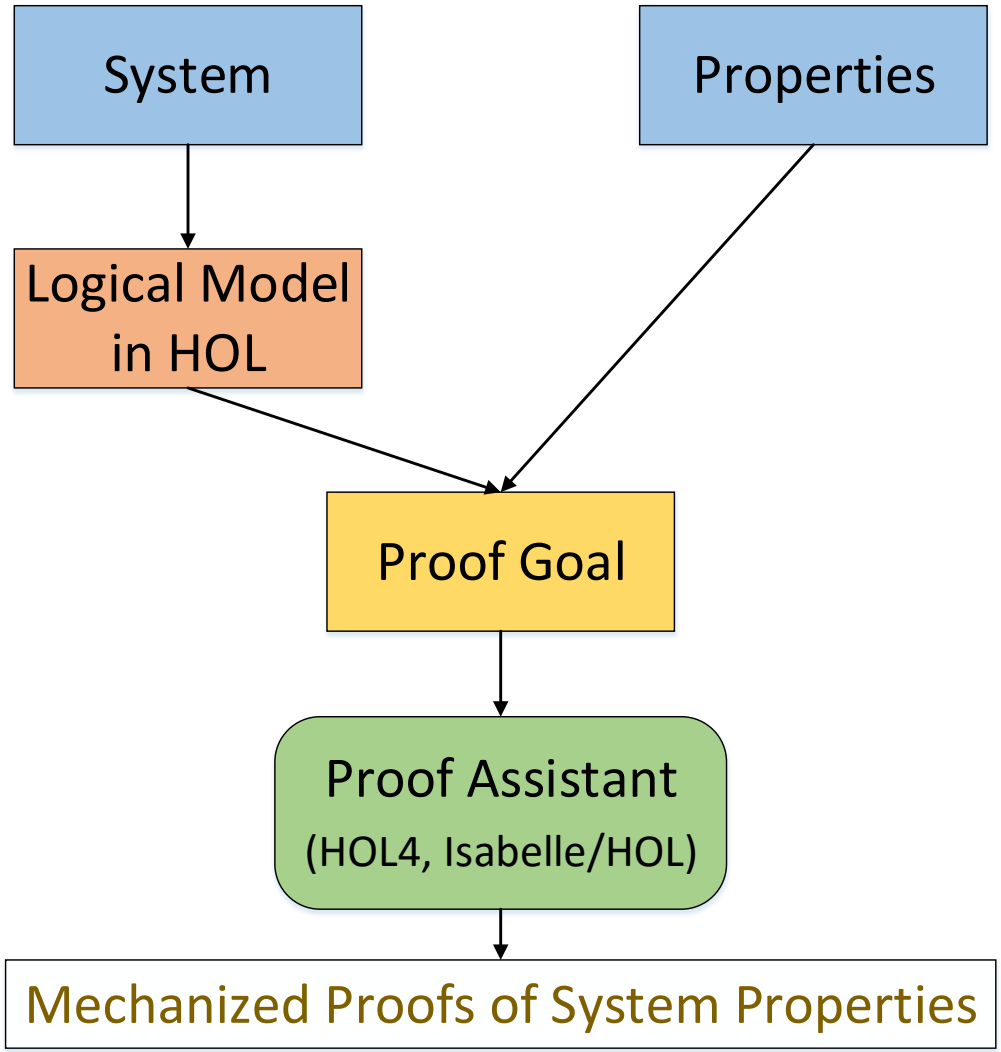
- Several Probabilistic and Statistical model checking tools have been used for reliability/availability assesment
  - Probabilistic model checker (PRISM) (Baier et al. MIT Press 2008)
  - COMPASS: Based on the NuSMV and Markov Chain model checker (MRMC) (Bozanno et al. SAFECOMP-2009)
  - Erlangen-Twente Markov Chain Checker (ETMCC) (Hermanns et al. DSN-2013)

Dependability Analysis using Model Checking

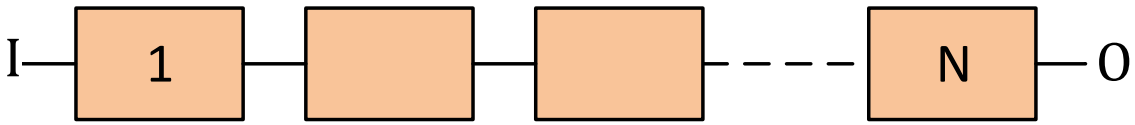
- Several Probabilistic and Statistical model checking tools have been used for reliability/availability assesment
  - Probabilistic model checker (PRISM) (Baier et al. MIT Press 2008)
  - COMPASS: Based on the NuSMV and Markov Chain model checker (MRMC) (Bozanno et al. SAFECOMP-2009)
  - Erlangen-Twente Markov Chain Checker (ETMCC) (Hermanns et al. DSN-2013)

- Analysis of Real-world systems
  - Aerospace systems (Bozanno et al. SAFECOMP-2009)
  - RAID disk protocol (Gopinath et al. Tech report 2009)
  - Herschel-Planck satellite system (Pend et al. Modeling Symp. 2013)
  - Airbag system (Pend et al. Modeling Symp. 2013)
  - e-health systems used in hospitals (Pervez et al. e-HEALTHCOMM-2014)

Higher-order-Logic Theorem Proving

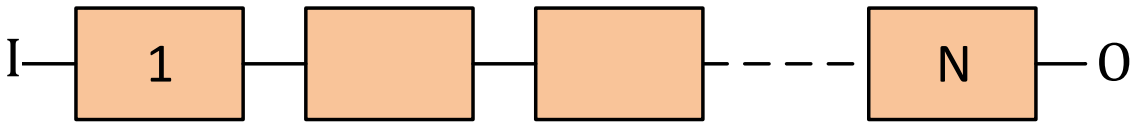


HOL Theorem Proving - Example: Series RBD



$$R_{series}(t) = Pr(\bigcap_{i=1}^{N} A_i(t)) = \prod_{i=1}^{N} R_i(t)$$

HOL Theorem Proving - Example: Series RBD

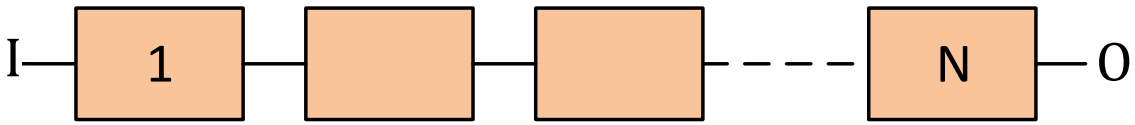


$$R_{series}(t) = Pr(\bigcap_{i=1}^{N} A_i(t)) = \prod_{i=1}^{N} R_i(t)$$

Definition: Series RBD

```
⊢ ∀ p L. series_struct p L = inter_list p L
```

HOL Theorem Proving - Example: Series RBD



$$R_{series}(t) = Pr(\bigcap_{i=1}^{N} A_i(t)) = \prod_{i=1}^{N} R_i(t)$$

Definition: Series RBD

$\vdash \forall$ p L. series_struct p L = inter_list p L

Theorem: Series RBD Reliability

$\vdash \forall$ p L. prob_space p $\wedge$ $\backsim$NULL L $\wedge$
mutual_indep p L $\wedge$ in_events p L $\Longrightarrow$
(prob p (series_struct p (rel_event_list p L t)) =
list_prod (list_prob p (rel_event_list p L t)))

Dependability Analysis using HOL Theorem Proving

- Probability Theory
  -  J. Hurd (2002), PhD Thesis, University of Cambridge
    Formal Verification of Probabilistic Algorithms.
  -  O. Hasan (2008), PhD Thesis, Concordia University
    Formal Probabilistic Analysis using Theorem Proving.
  -  T. Mhamdi (2011), PhD Thesis, Concorida University
    Information-Theoretic Analysis using Theorem Proving.
  -  J. Hölzl (2012), PhD thesis, Technical University of Munich
    Construction and Stochastic Applications of Measure Spaces in Higher-Order Logic.

Dependability Analysis using HOL Theorem Proving

- Dependability Analysis of a Component
  - Reconfigurable Memory Arrays (Hasan et al. TC-2010)
  - Combinational Circuits (Hasan et al. JAL-2011)
  - Electronic System Components (Abbasi et al. WoLLIC-2014

Dependability Analysis using HOL Theorem Proving

- Dependability Analysis of a Component
  - Reconfigurable Memory Arrays (Hasan et al. TC-2010)
  - Combinational Circuits (Hasan et al. JAL-2011)
  - Electronic System Components (Abbasi et al. WoLLIC-2014
- Dependability Analysis using RBDs and FTs
  - Oil and Gas Pipelines (Waqar et al. CICM-2014)
  - WSN Transport Protocols (Waqar et al. WiMob-2015)
  - Logistic Supply Chain (Waqar et al. IWIL-2015)
  - Satellite Solar Array (Waqar et al. CICM-2015)

Comparison between Dependability Analysis Techniques

Feature	Paper-and-pencil Proof	Simulation Tools	Petri Nets	Theorem Proving	Model Checking

Comparison between Dependability Analysis Techniques

Feature	Paper-and-pencil Proof	Simulation Tools	Petri Nets	Theorem Proving	Model Checking
Expressiveness	✓	✓		✓	

Comparison between Dependability Analysis Techniques

Feature	Paper-and-pencil Proof	Simulation Tools	Petri Nets	Theorem Proving	Model Checking
Expressiveness	✓	✓		✓	
Accuracy	✓ (?)		✓	✓	✓

Comparison between Dependability Analysis Techniques

Feature	Paper-and-pencil Proof	Simulation Tools	Petri Nets	Theorem Proving	Model Checking
Expressiveness	✓	✓		✓	
Accuracy	✓ (?)		✓	✓	✓
Automation		✓	✓		✓

Outline

Conclusion

- Dependability
  - Reliability
  - Availability
  - Maintainability

Conclusion

- Dependability
  - Reliability
  - Availability
  - Maintainability

- Dependability Modeling Techniques
  - Reliability Block Diagram
  - Fault Tree
  - Markov Chains

Conclusion

- Dependability
  - Reliability
  - Availability
  - Maintainability
- Dependability Modeling Techniques
  - Reliability Block Diagram
  - Fault Tree
  - Markov Chains
- Formal Dependability Analysis Techniques
  - Petri Nets
  - Model Checkng
  - Interactive Theorem Proving

Timeline of Surveyed Papers

	Before 1990s	1990-99	2000-09	2010-16

Timeline of Surveyed Papers

	Before 1990s	1990-99	2000-09	2010-16
Introduction of Models	RBDs and FTs	Markov Chains	Dynamic RBDs and FTs	

Timeline of Surveyed Papers

	Before 1990s	1990-99	2000-09	2010-16
Introduction of Models	RBDs and FTs	Markov Chains	Dynamic RBDs and FTs	
Introduction of Analysis Techniques		Petri Nets	Model Checking	Theorem Proving

Timeline of Surveyed Papers

	Before 1990s	1990-99	2000-09	2010-16
Introduction of Models	RBDs and FTs	Markov Chains	Dynamic RBDs and FTs	
Introduction of Analysis Techniques		Petri Nets	Model Checking	Theorem Proving

Future Directions:

- Analysis of Dynamic RBDs and FTs
- Using Theorem Proving to conduct Markov Chains based dependability analysis
  - Foundational Support is available in HOL4 (L. Liu et al., ATVA-2011) and Isabelle/HOL (J. Hölzl et al., TACAS 2012)

Thanks!

save.seecs.nust.edu.pk