Reliability Block Diagrams based Analysis: A Survey

O. Hasan[1], W. Ahmed[1] S. Tahar[2] and M.S. Hamdi[3]

[1]National University of Sciences and Technology, Islamabad Pakistan
[2]Concordia University, Montreal, Canada
[3]Ahmed Bin Mohammed Military College, Doha, Qatar

ICNAAM 2014
Rhodes, Greece

Outline

- Reliability Block Diagrams
- Analysis Techniques
  - Example: RBD based Analysis of a simple Oil and Gas Pipeline
- Conclusions

Reliability

- A measure of the continuity of service
- Probability that a system performs its intended function until some time t without failing

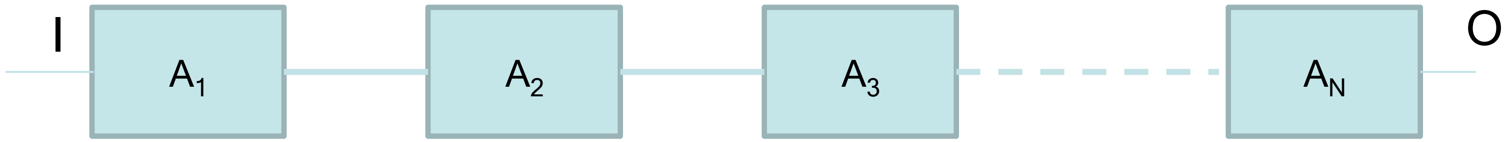
$$R(t) = Pr(X > t) = 1 - Pr(X \leq t) = 1 - F_X(t)$$

- X: random variable that models the time to failure of the system
  - Commonly used Distributions
    - Exponential
    - Weibul

Reliability Block Diagrams

- Used to asses the reliability of a complex system
  - Partition the system into sub-blocks and connectors (RBD)
  - Find the failure rates of sub-blocks
  - Judge the failure characteristics of the overall system
    - failure rates of individual components
    - RBD configuration
- The overall system failure happens if all the paths for successful execution fail
  - Add more parallelism to meet the reliability goals

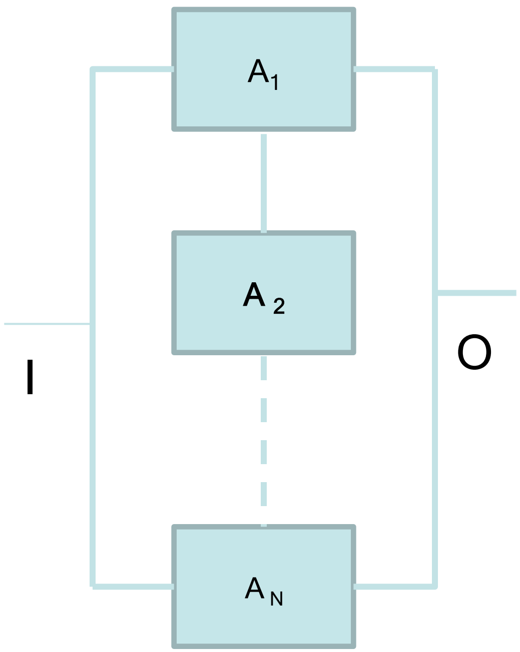
Series Reliability Block Diagram



- The overall system is reliable only if all of its components are functioning reliably
- If $A_i(t)$ are the mutually independent events corresponding to *i serially-connected* components then

$$R_{series}(t) = Pr(A_1(t) \cap A_2(t) \cap A_3(t) \cdots \cap A_N(t)) = \prod_{i=1}^{N} R_i(t)$$

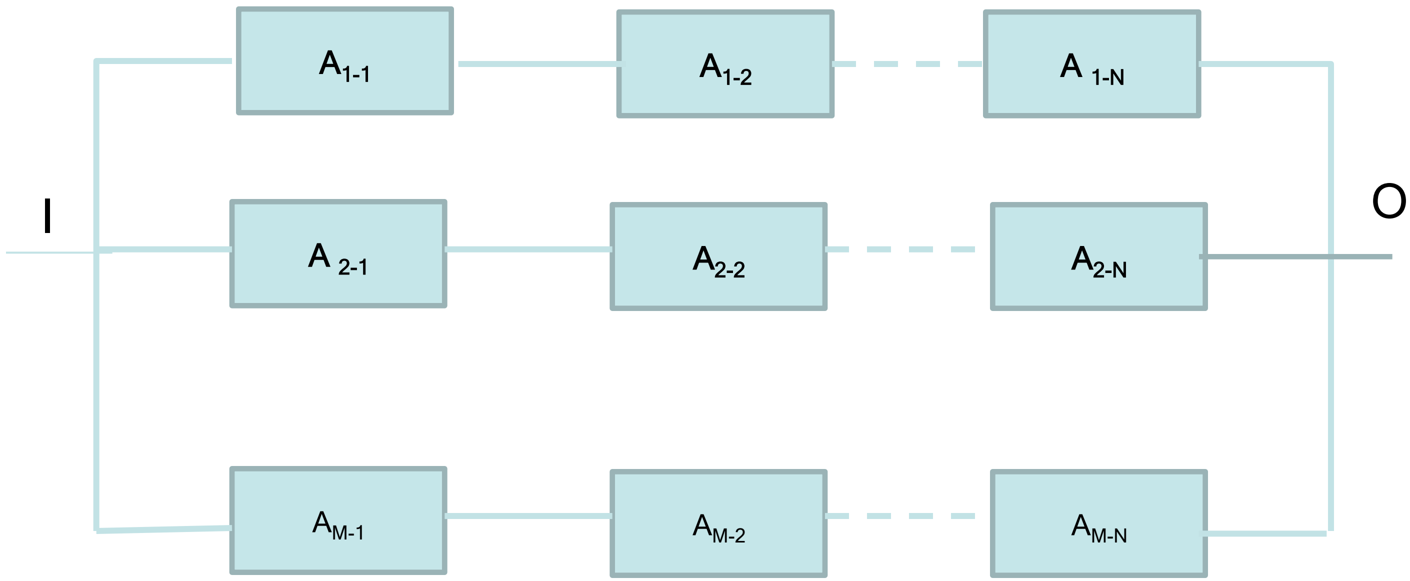
Parallel Reliability Block Diagrams



- The overall system reliability mainly depends on the component with the maximum reliability
- If $A_i(t)$ are the mutually independent events corresponding to *i* *parallel-connected* components then

$$R_{parallel}(t) = Pr(A_1 \cup A_2 \cup A_3 \cdots \cup A_N) = 1 - \prod_{i=1}^{N}(1 - R_i(t))$$

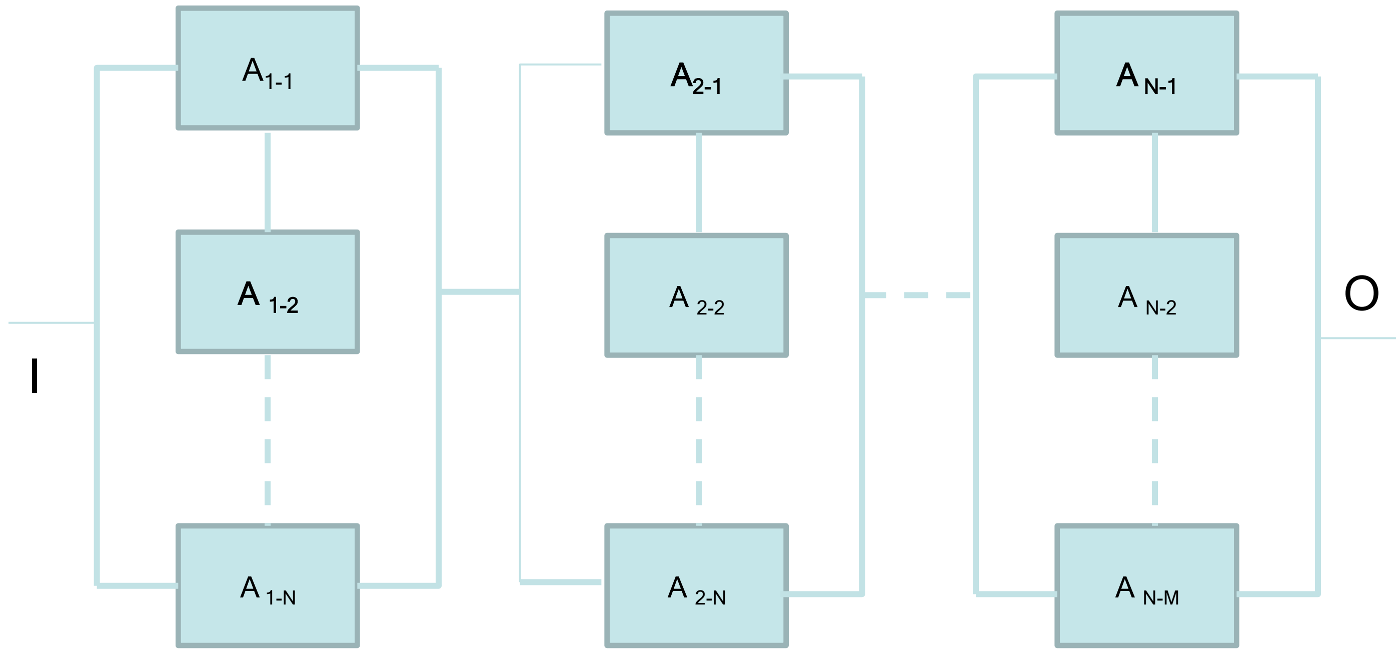
Series-Parallel Reliability Block Diagrams



- A combination of both series and parallel RBD

$$R_{Series-Parallel} = Pr(\bigcap_{i=1}^{N} \bigcup_{j=1}^{M} A_{ij}) = \prod_{i=1}^{N} (1 - \prod_{j=1}^{M} (1 - R_{ij}(t)))$$

Parallel- Series Reliability Block Diagrams



$$R_{Parallel-Series} = Pr(\bigcup_{i=1}^{M} \bigcap_{j=1}^{N} A_{ij}) = 1 - \prod_{i=1}^{M} (1 - \prod_{j=1}^{N} (R_{ij}(t)))$$

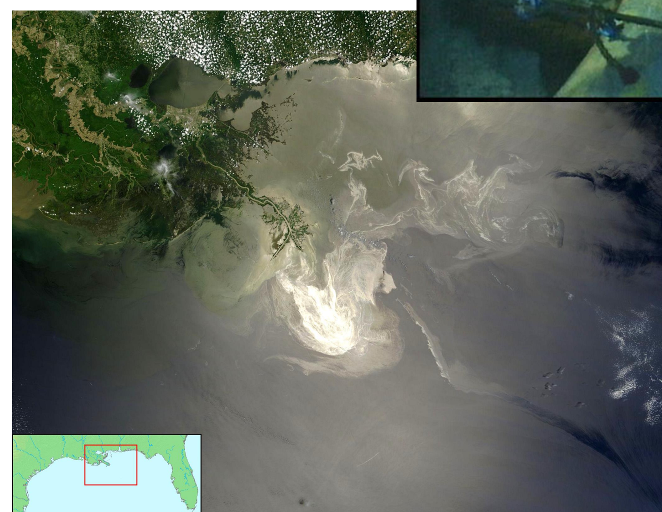
Example: Reliability Analysis of Oil and Gas Pipelines

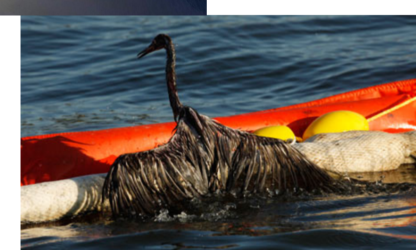
- There are tens of thousands of miles long oil and gas pipelines around the world
  - Some of them aging and are becoming more and more susceptible to failures

- Very important to rigorously analyze their reliability and thus plan timely replacements and maintenance

Methane Gas Leakage on the Deepwater Horizon oil rig – April 2010

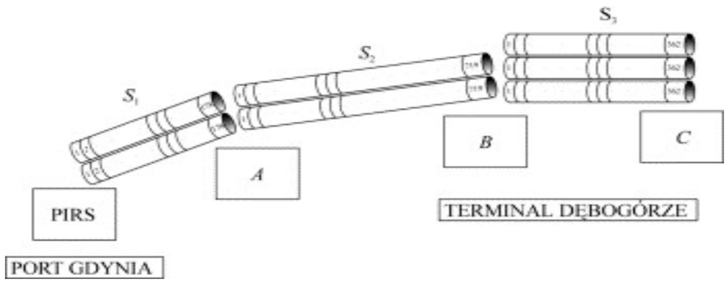
- Killed 11 workers
- Destroyed and sank the rig
- Caused millions of gallons of oil to pour into the Gulf of Mexico
- Took three months to bring the situation under control
- Damage to marine and wildlife habitats

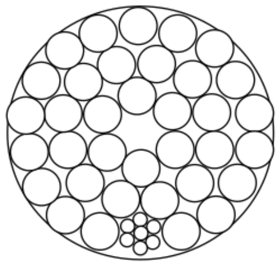


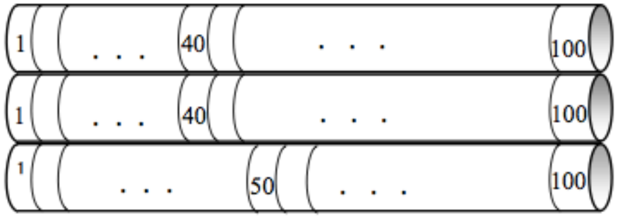


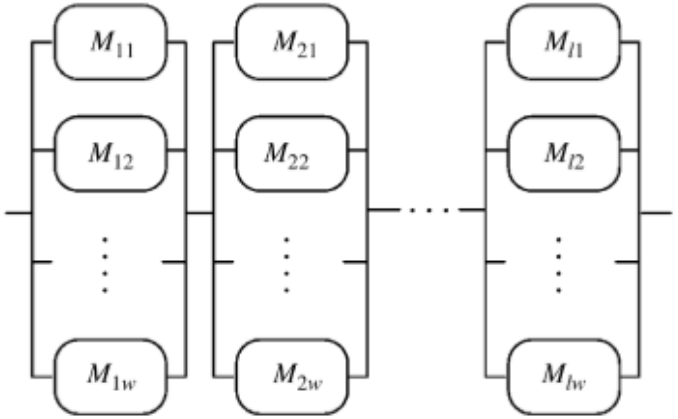
Reliability Analysis of Pipelines

- Partitioning the given pipeline into segments and constructing its equivalent reliability block diagram (RBD)









RBD Analysis Techniques

- Paper-and-Pencil Proof Methods
- Simulation
- Theorem Proving

Paper-and-Pencil Proof Methods

- Construct a RBD of the given system on Paper
- Analytically analyze the overall reliability of the given system on paper
  - Already verified RBD relationships
  - Distribution functions of the failure modeling random variables

- Error Prone
  - Manual manipulation and simplification
  - Missing assumptions

Computer Simulations

- Generate samples from the Exponential and Weibull random variables to model the reliabilities of the sub-modules
- Compute the overall reliability of the given system based on the already verified RBD relationships

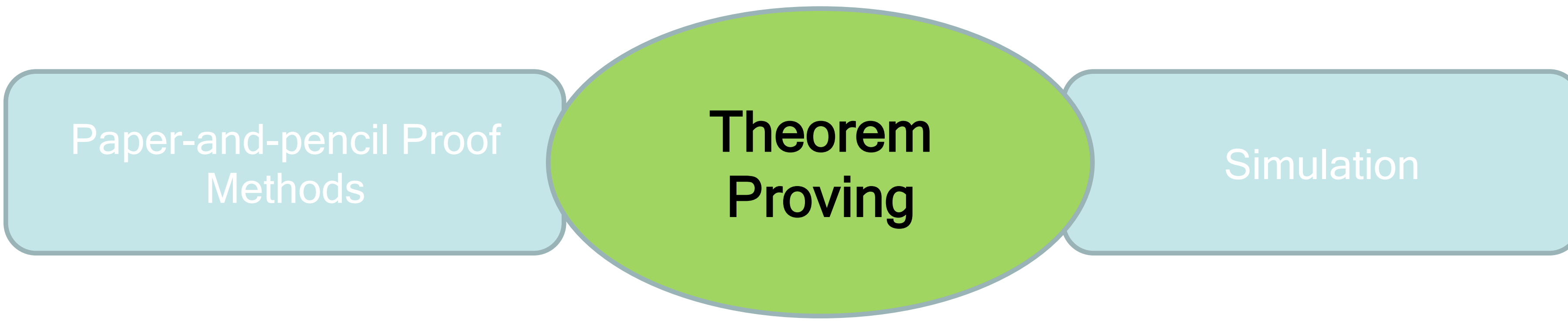
- Error Prone
  - Pseudo random Numbers
  - Computer arithmetic
  - Numerical techniques

Inaccuracies in RBD based analysis

- A severe limitation in the case of safety-critical applications like oil and gas pipelines
  - May endanger human and animal life
  - Lead to a significant financial loss

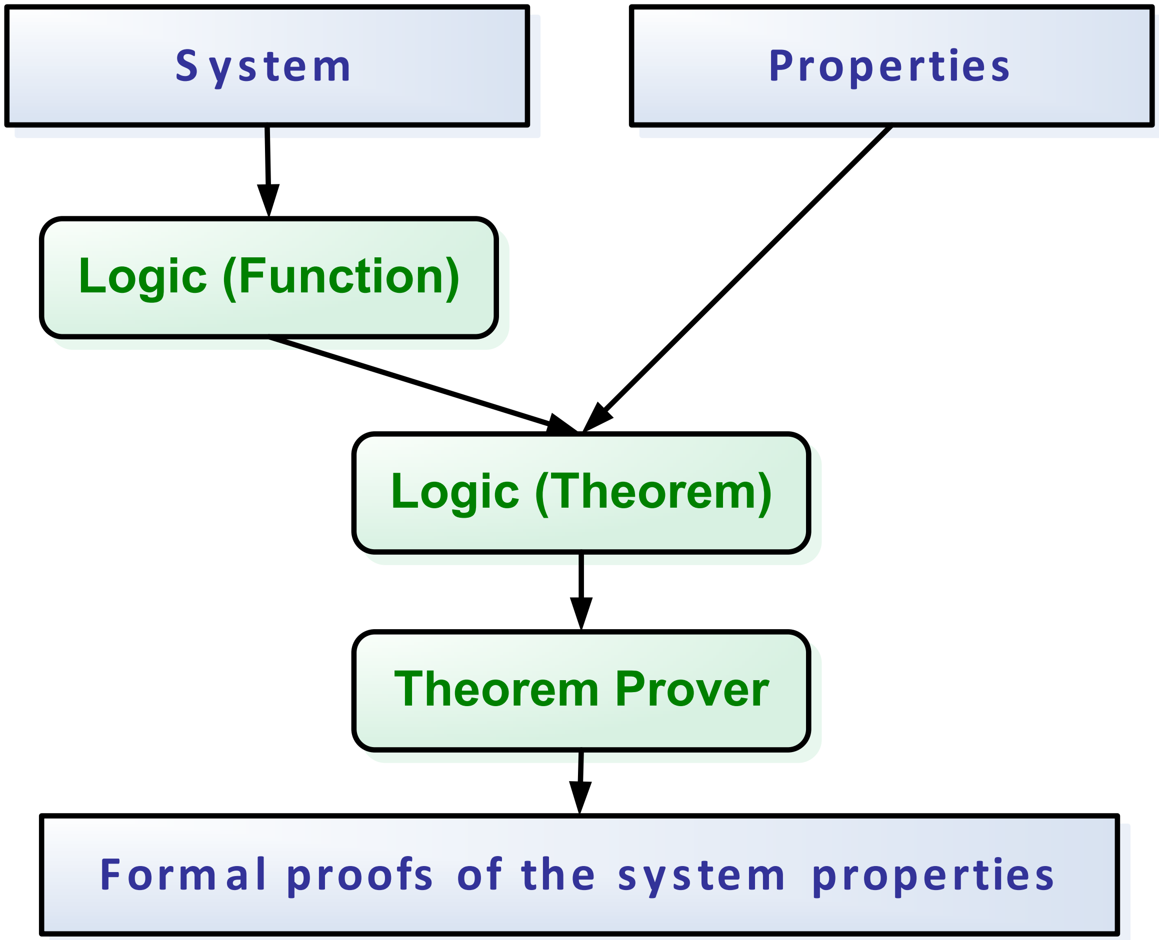
Theorem Proving

- Bridges the gap between Paper-and-pencil proof methods and simulation



- Shares their advantages
  - As precise as a mathematical proof can be
  - Computers are used for book-keeping
- Not as straightforward to use as simulation

Theorem Proving



Logic

- Study of drawing conclusions (reasoning)
  - Propositional logic
    - Supports statements that can be true or false
  - First-order logic (Predicate logic)
    - Quantification over variables (∀: For all, ∃: there exists)
  - Higher-order logic
    - Quantification over sets and functions

Propositional Logic → First-Order Logic → Higher-Order Logic

Less expressive(-) → Very expressive(+)

Decidable(+) → Undecidable(-)

Theorem Prover

- A theorem prover consists of
  - A notation (Syntax)
  - A small set of fundamental axioms (facts)
    - Example: $(\neg\neg A) \Leftrightarrow A$
  - A small set of deduction rules
    - Example: Given $(A \rightarrow B)$ and A, we can deduce B
- Soundness is assured as every new theorem must be created from
  - The basic axioms and primitive inference rules
  - Any other already proved theorems (Theory Files)

Theorem Proving - Example: Natural Log of Product

```
val LN_MUL = store_thm("LN_MUL",
  (--`∀x y. 0 < x ∧ 0 < y ⇒ (ln (x * y) = ln x + ln y)`--),

REPEAT GEN_TAC THEN STRIP_TAC THEN
ONCE_REWRITE_TAC[GSYM EXP_INJ] THEN
REWRITE_TAC[EXP_ADD] THEN
SUBGOAL_THEN (--`&0 < x * y`--) ASSUME_TAC THENL
  [MATCH_MP_TAC REAL_LT_MUL THEN ASM_REWRITE_TAC[],
   EVERY_ASSUM(fn th => REWRITE_TAC[ONCE_REWRITE_RULE[GSYM EXP_LN]
th])]);
```

[EXP_INJ] ∀x y. (exp x = exp y) ⇔ (x = y)

[EXP_ADD] ∀x y. exp (x + y) = exp x * exp y

[EXP_LN] ∀x. (exp (ln x) = x) ⇔ 0 < x

Formal Reliability Analysis - Requirements

- Formalization of Probability Theory is the foremost requirement for reliability analysis

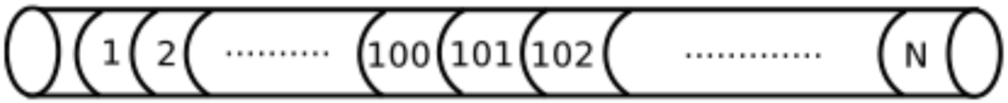
- Formalization of Continuous Random Variables

- Recursive Definitions for Reliability Block Diagrams

Have to use a Higher-order Logic Theorem Prover

Formal Reliability Analysis of a Simple Oil and Gas Pipeline using Theorem Proving - CICM 2014

- Formalization of Reliability in HOL
- Formalization of Series RBD in HOL
- Formal RBD based analysis of a simple pipeline



- Generic expressions involving
  - any number of segments
  - arbitrary failure rates
  - All assumptions are explicitly available

Summary

Criteria	Paper-and-Pencil Proof	Simulation	Higher-order-logic Proof Assistants
Expressiveness	✓	✓	✓
Accuracy	✓ ?	✗	✓
Automation	✗	✓	✗ ✓

- The precision of results is very important while analyzing safety-critical domains
- Theorem Proving can guarantee precise reliability analysis

Future Recommendations

- Formalization of other RBDs
  - Parallel, series-parallel and parallel-series
- More case studies
  - Virtual Data Centers
  - More complex Pipelines

Thanks!

- For More Information
  - Visit our website
    - http://save.seecs.nust.edu.pk
  - Contact
    - osman.hasan@seecs.nust.edu.pk