Digital Design and Dependability Research Group

# Pessimistic Dependability Models Based on Hierarchical Markov Chains

Martin Kohlík, Hana Kubátová

martin.kohlik@fit.cvut.cz, hana.kubatova@fit.cvut.cz

CTU in Prague

# Outline

- Motivation
- Dependability Models Reduction
- Hierarchical Markov Chain Models
- Partial Reduction
- Conclusions

# Motivation

- What?
  - To calculate dependability parameters of complex systems based on dependable blocks
- Why?
  - To prove that our dependable designs can be used as railway equipment
- How?
  - Hierarchical dependability models based on Markov chains are used
  - Total hazard rate of the system is calculated

# Motivation

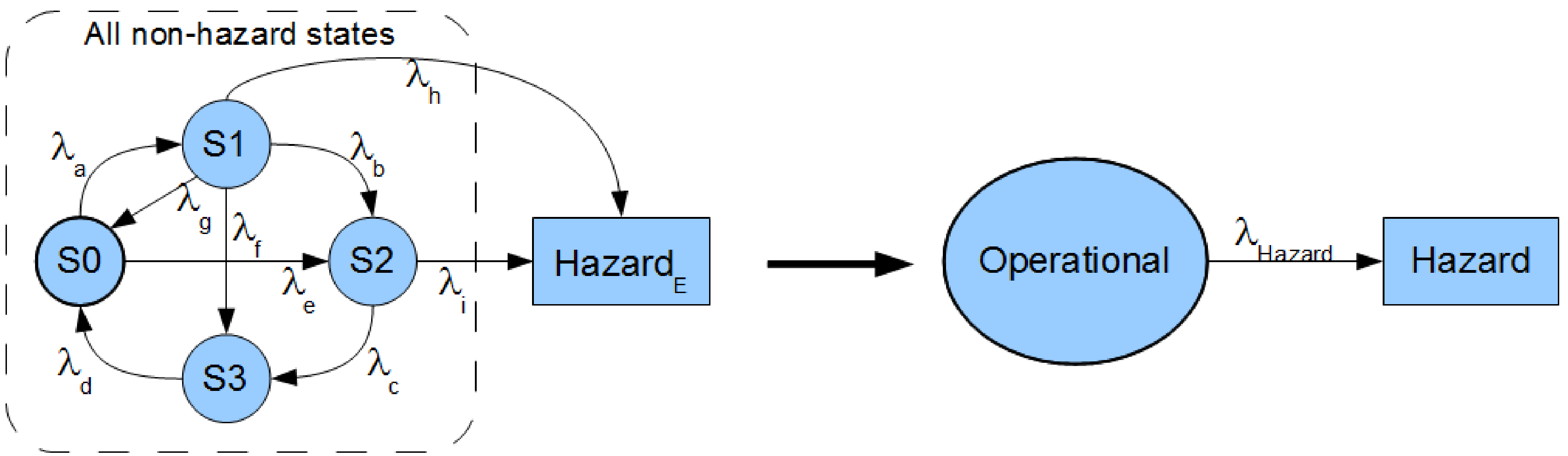
- Simple dependability models
  - Easy to understand
  - Does not reflect the internal structure of the design

**VS.**

- Complex dependability models
  - More accurate
  - Grows rapidly in size
  - Complicated to read and modify

# Dependability Models Reduction
## Introduction

- Intended for non-renewable Markov chains
- Results into one hazard rate and its exponential failure distribution function (F(t))
- Inexact, but pessimistic



# Dependability Models Reduction

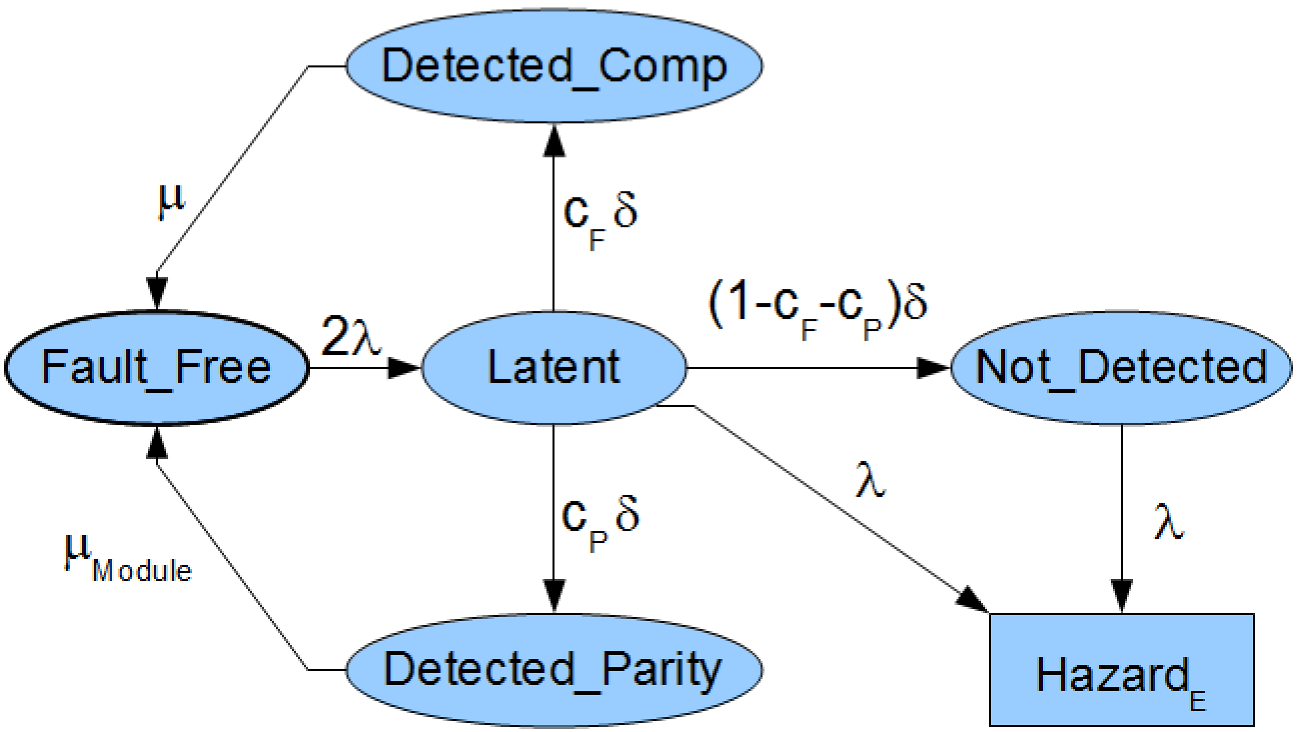
## Steps

- Calculate the exact failure distribution function
- Find an estimated hazard rate value
  - Fast estimation
  - The starting point of the next step
- Correct an estimated hazard rate to get pessimistic values
  - Find the lowest value
  - Numeric method meeting the required accuracy

# Dependability Models Reduction

## Case study

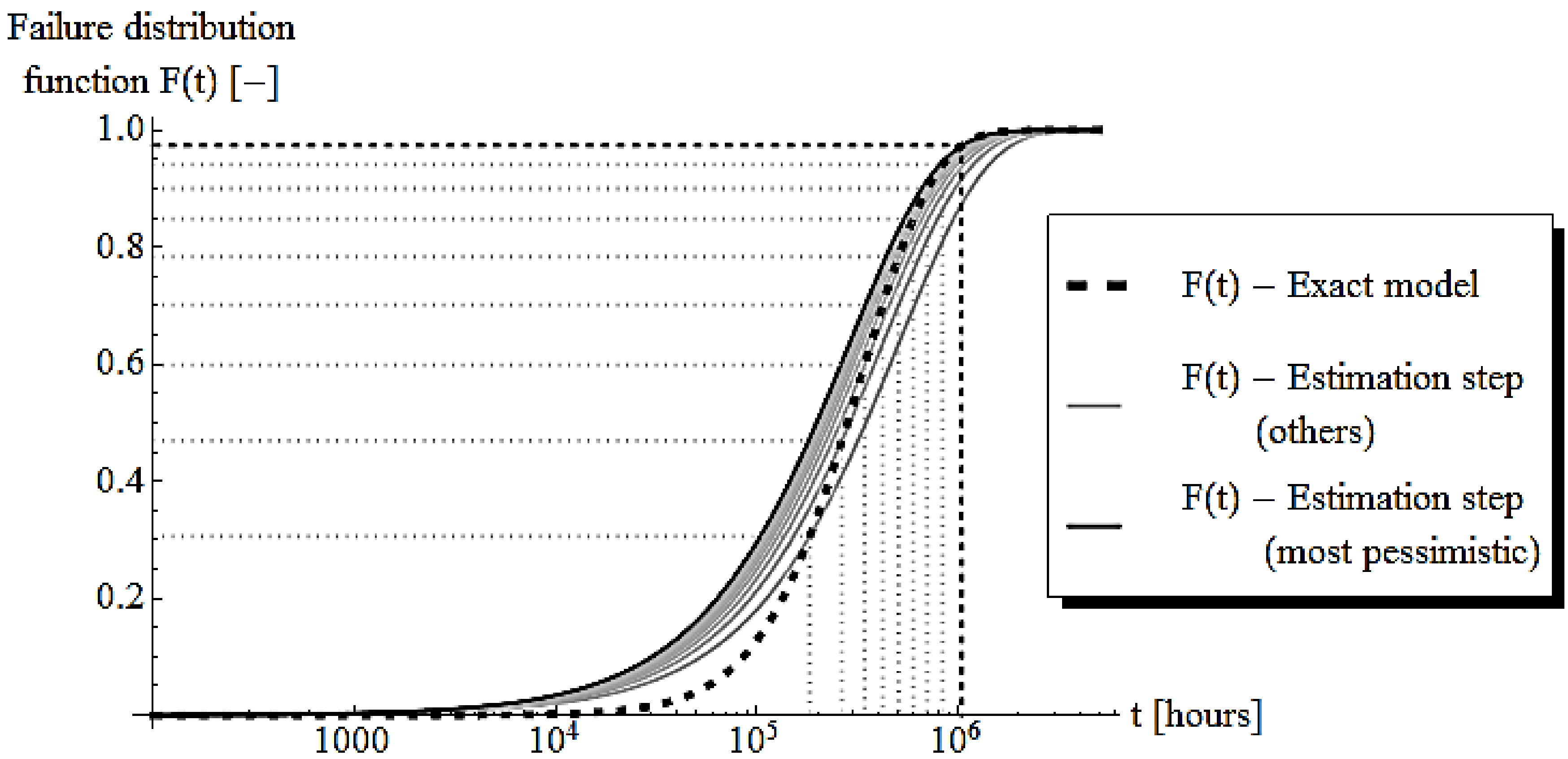
- Modified Duplex System (MDS)
  - Based on two independent modules with parity checkers attached
  - Able to detect faults by parity checkers and by comparators



# Dependability Models Reduction

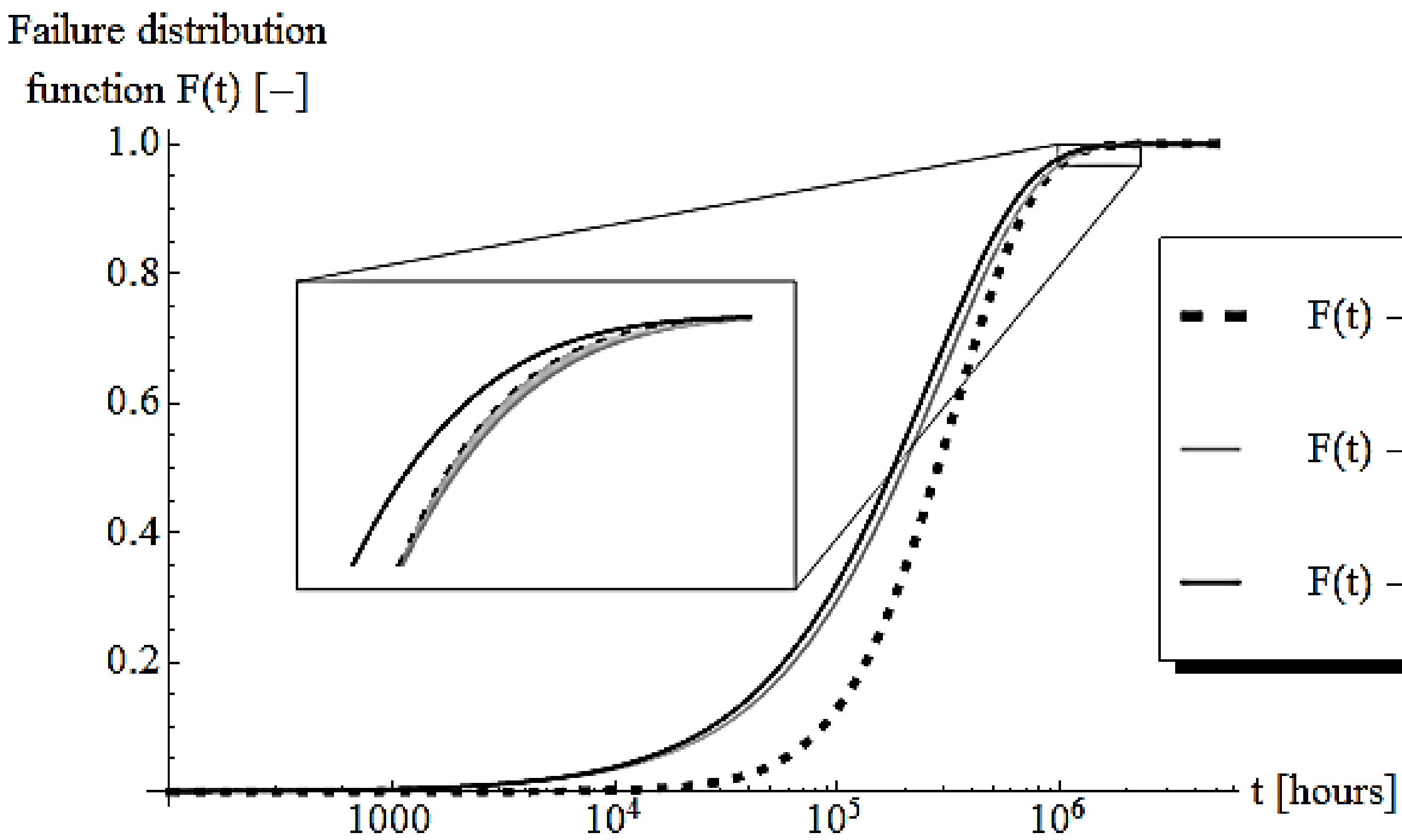
## Case study

- Estimation step



# Dependability Models Reduction
## Case study

- Correction step



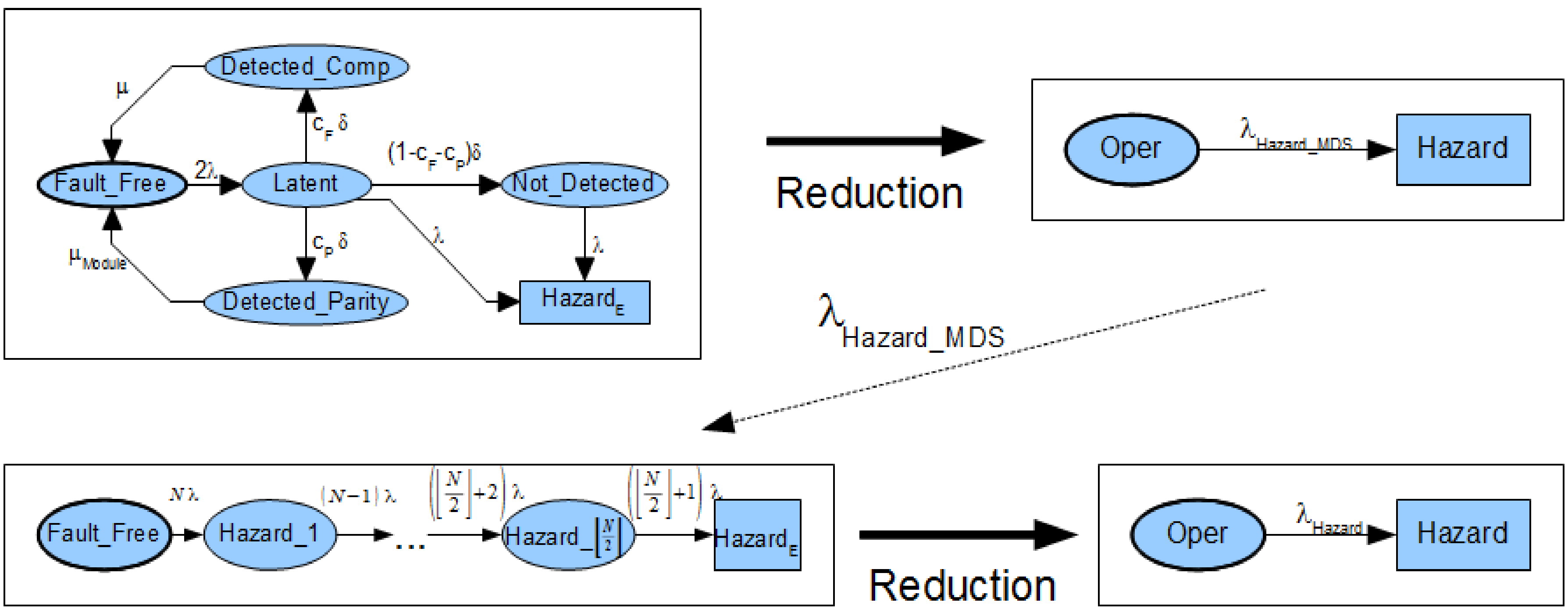
# Hierarchical Markov Chain Models
## Introduction

- Allow modeling advanced redundancy techniques of the blocks in the same way as Markov chains
- Allow separate calculations of low- and high-level models
- Allow avoidance of the state explosion

# Hierarchical Markov Chain Models
## Case study

- Case study system
  - Up to 17 identical dependable blocks (Modified Duplex System – MDS)
  - N-modular redundant system (NMR) configuration
  - Classic complex model
    - Up to cca. 25000 states
  - Hierarchical Model
    - 2 linked models
      - top NMR model – up to 10 states
      - a model of the block – 6 states

# Hierarchical Markov Chain Models
## Case study



# Hierarchical Markov Chain Models

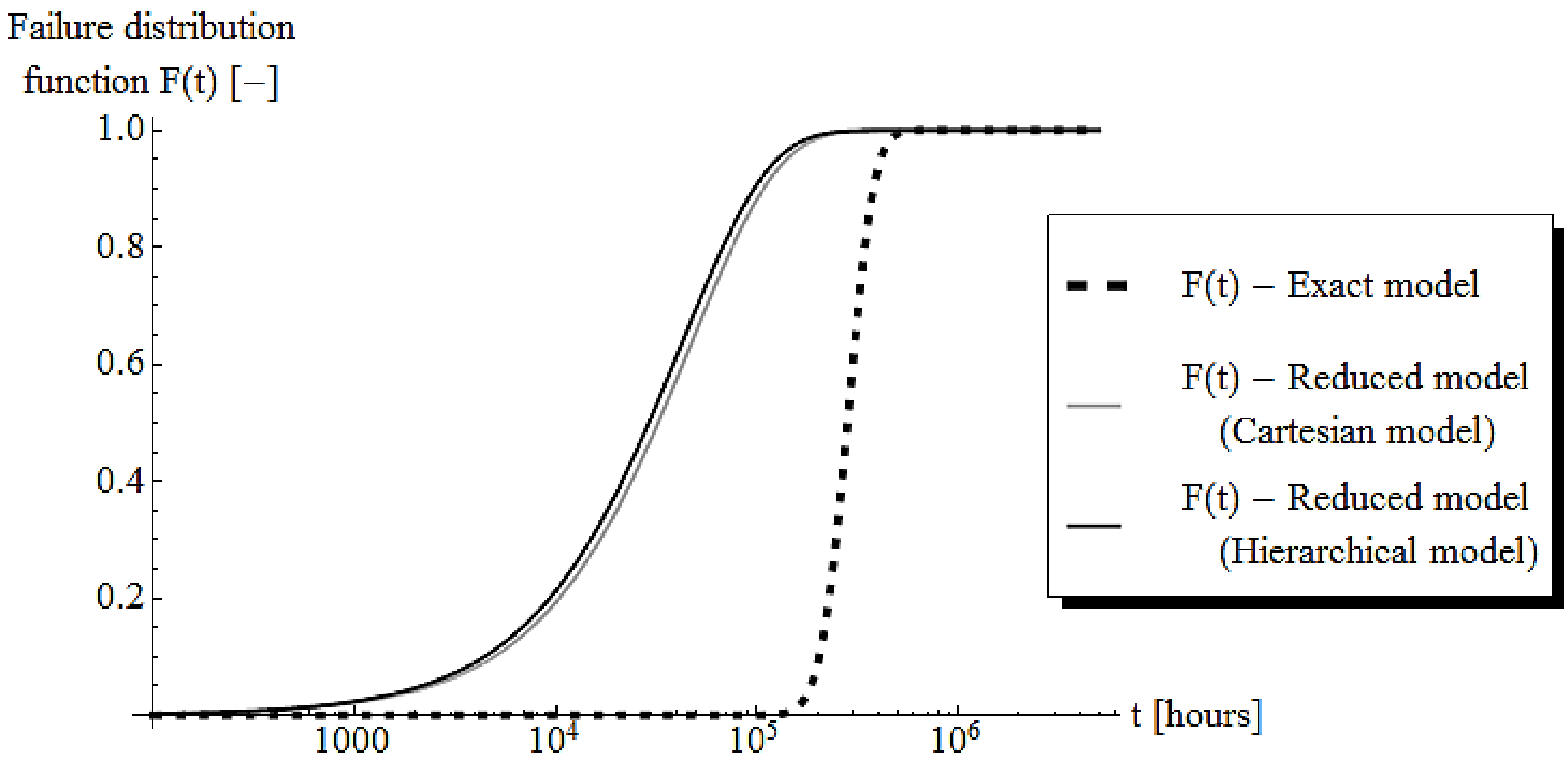
## Case study – Results

| NMR blocks | No. of states | Exact solution [s] | Hierarchical solution [s] |
|---|---|---|---|
| n1(MDS) | 6 | 0.016 | 0.139 |
| n3 | 55 | 0.062 | 0.251 |
| n5 | 246 | 0.218 | 0.248 |
| n7 | 771 | 0.671 | 0.247 |
| n9 | 1,946 | 2.590 | 0.247 |
| n11 | 4,242 | 8.830 | 0.250 |
| n13 | 8,316 | 24.24 | 0.246 |
| n15 | 15,042 | 96.58 | 0.252 |
| n17 | 25,542 | 391.7 | 0.255 |
| | | … | |
| n99 | - | ca. $10^{17}$ years* | 0.248 |

# Hierarchical Markov Chain Models

## Case study – Results

- NMR17 system results



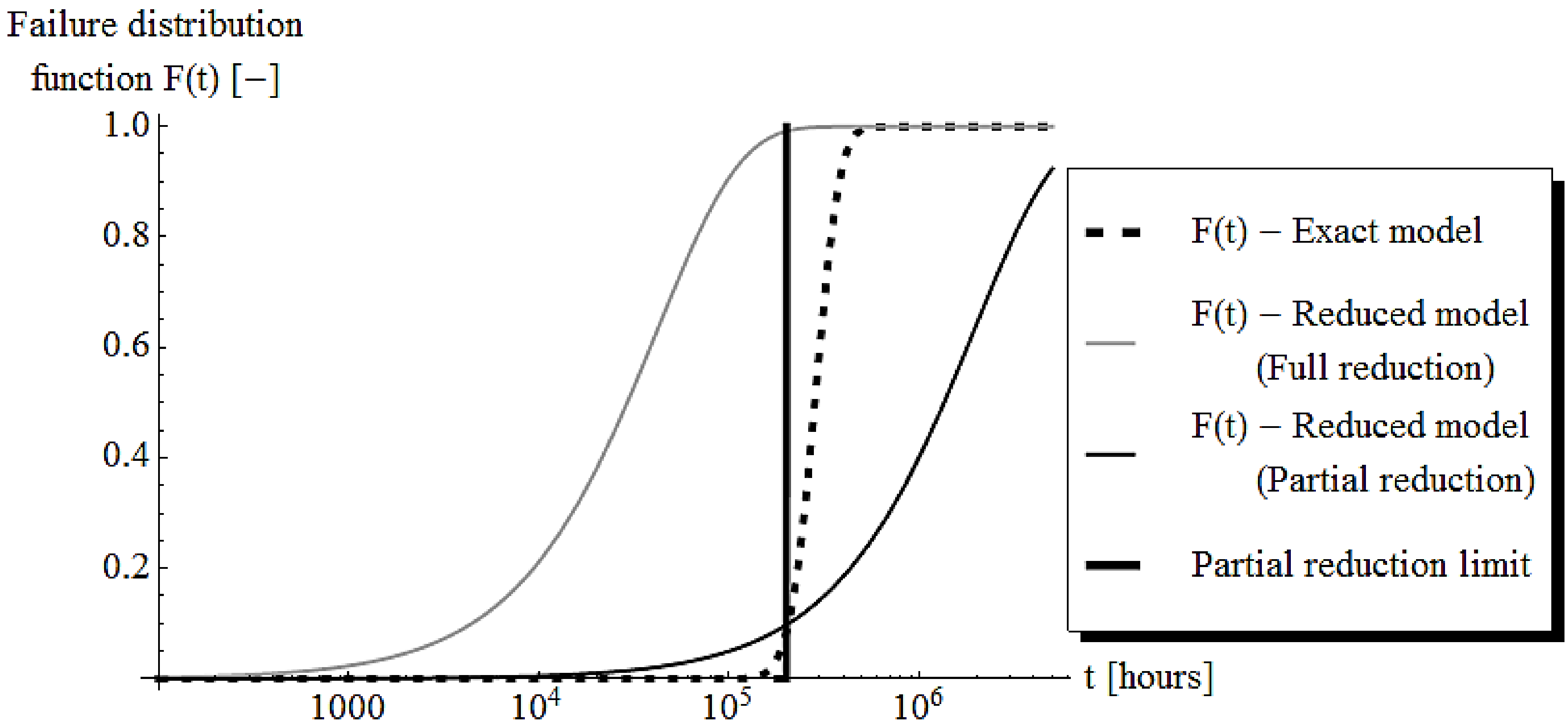
# Partial reduction
## Introduction

- Pessimistic until specified time or probability limit value
  - Result hazard rate cannot be used beyond this limit value
  - Provides maximal operational time (warranty period) of the system
- More accurate
- Same speedup as unlimited method

# Partial reduction

## Case study – Time limited results

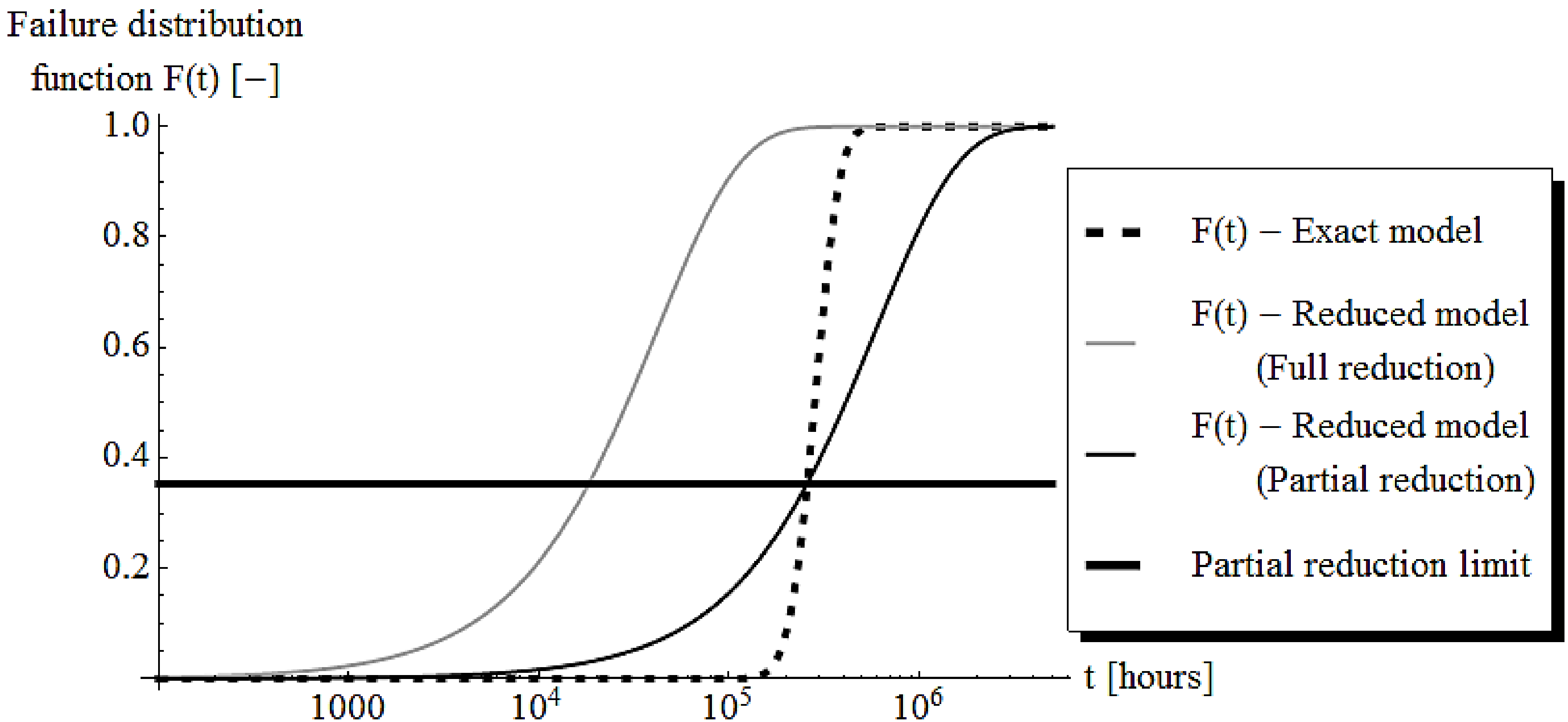
- NMR17 system results – $t_{limit}$ = 200,000 hours (ca. 22 years)
- Hazard rates: $23.8 \times 10^{-6}$ vs. $0.5 \times 10^{-6}$ (ca. 40x lower)



# Partial reduction

## Case study – Probability limited results

- NMR17 system results – $p_{limit} = 0.35$
- Hazard rates: $23.8 \times 10^{-6}$ vs. $1.6 \times 10^{-6}$ (ca. 15x lower)



# Conclusions

- Reduction of Markov chains
  - Intended for non-renewable Markov chains
  - Inexact, but pessimistic
  - Results into one hazard rate and its failure distribution function (F(t))
- The hierarchical dependability models
  - Based on Markov chains and reduction
  - Nearly constant reduction time (vs. exponential grow with the number of low-level blocks in exact model)
- Partial reduction
  - More accurate
  - Same speedup as unlimited reduction
  - Provides maximal operational time (warranty period) of the system
  - Can be modified to be limited by the prescribed hazard rate