Mean Time To Failure

Lower-Bounding the MTTF for systems with (m,k) constraints and IID iteration failure probabilities

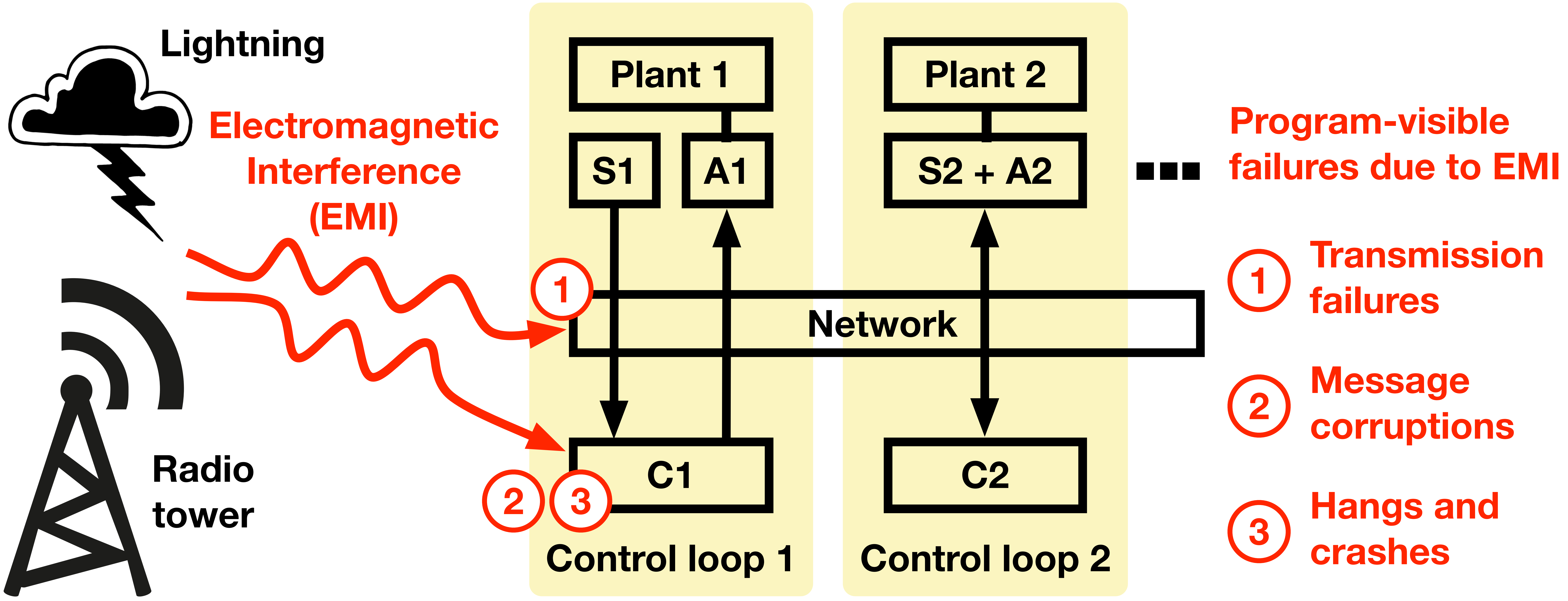
Independent and Identically Distributed

Arpan Gujarati,
Mitra Nasri, Björn B. Brandenburg

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

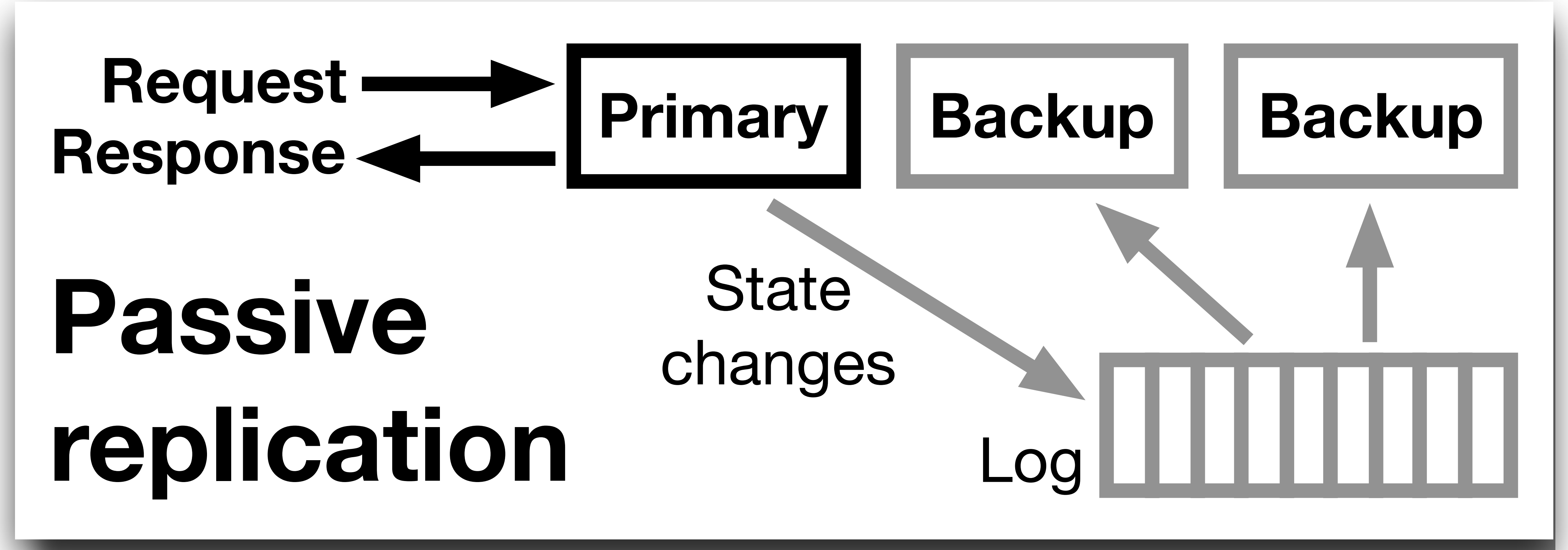
Reliability analysis of Networked Control Systems (NCS)

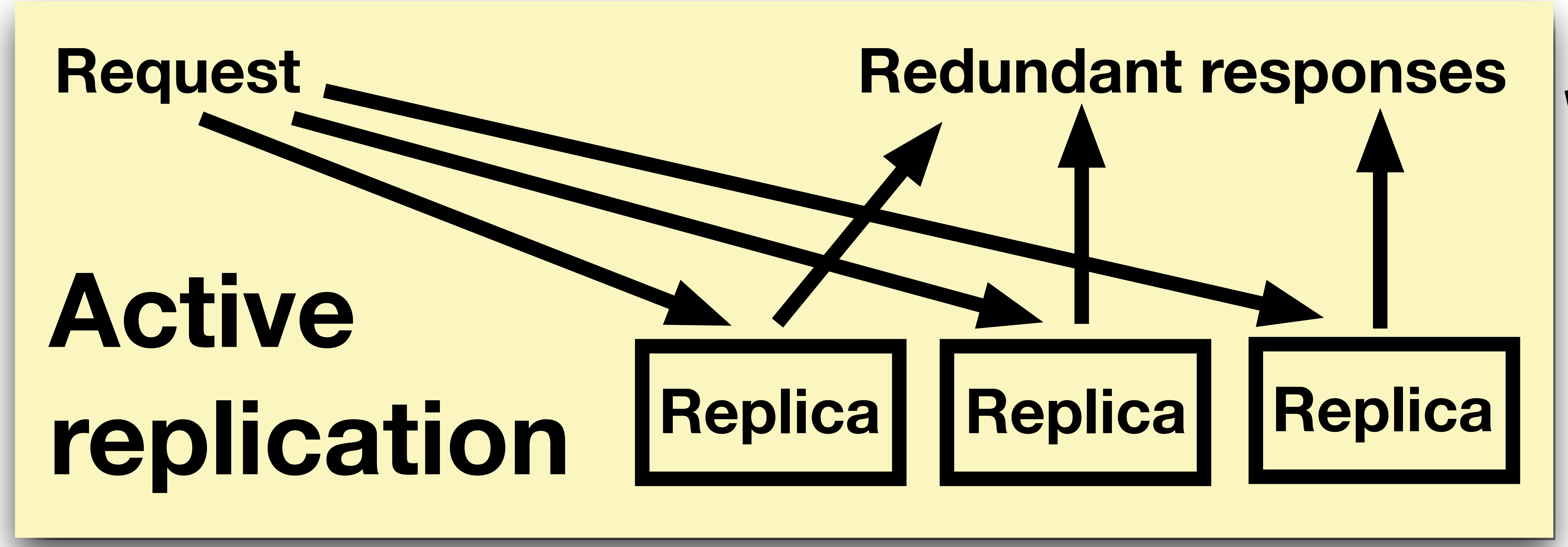
= multiple feedback control loops + distributed hosts
+ shared communication network



Safety-critical NCS must be fail-operational

i.e., continue functioning despite EMI-induced failures





Active replication is often used because...

A. NCSs are time-sensitive

B. they contain high-frequency control loops

Problem

What is a good active replication scheme?

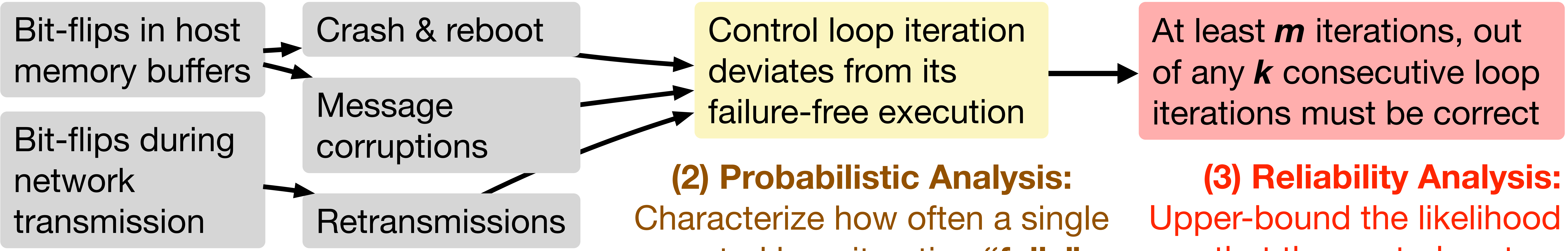
Constraints: size, weight, power, and cost

Objective: meet the dependability requirements

Opportunity: controller inherently robust to occasional disturbances

Quantifying NCS resiliency to EMI-induced transient faults

… to provide engineers with an objective metric for comparing different active replication schemes



(1) Fault Modeling: Transient faults modeled using **Poisson** distribution, empirically-derived **peak EMI** rates

(2) Probabilistic Analysis: Characterize how often a single control loop iteration **"fails"**

(3) Reliability Analysis: Upper-bound the likelihood that the control system **"fails beyond recovery"**

This probability is upper-bounded by **F**, which satisfies the **IID** property w.r.t. each iteration

(under submission)

Quantifying NCS resiliency to EMI-induced transient faults

… to provide engineers with an objective metric for comparing different active replication schemes

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

violation of the *(m,k)* constraint

Given F, lower-bound the Mean Time To Failure (MTTF)

(3) Reliability Analysis:

Upper-bound the likelihood that the control system **"fails beyond recovery"**

Given F, lower-bound the mean time to failure (MTTF)

Outline

1 Discrete probability density function (dPDF)

g(n) = P(first (m,k) violation in the n^{th} *iteration)*

2 Probability density function (PDF)

f(t) = P(first (m,k) violation at time t)

3 Mean time to failure (MTTF)

MTTF = E [system lifetime] = $\int_0^\infty t f(t)\, dt$

4 Evaluation

Failure = Violation of the (m,k) constraint:

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

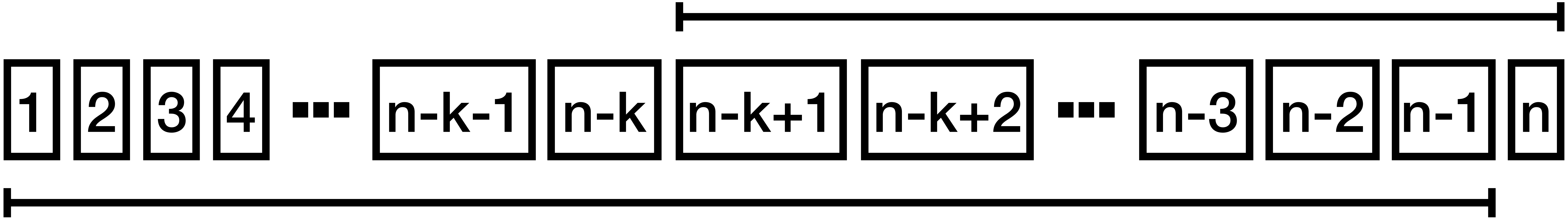
Lower-bounding dPDF (1/3)

g(n) = P(first (m,k) violation in the n^{th} iteration)

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

$$P(C1) = \binom{k-1}{k-m} F^{(k-m+1)}(1-F)^{m-1}$$

C1: Less than *m* correct iterations out of last *k* iterations



C2: *(m,k)* constraints not violated any time before the *n^{th}* iteration

Computationally challenging $P(C2) = ?$

Requires evaluating all possible combinations of failed and successful iterations among the first *n – 1* iterations.

Lower-bounding dPDF (2/3)

1 | 2 | 3 | 4 | ··· | n-k-1 | n-k | n-k+1 | n-k+2 | ··· | n-3 | n-2 | n-1 | n

C2: *(m,k)* constraints not violated any time before the n^{th} iteration

Computationally challenging

$$P(C2) = ?$$

Requires evaluating all possible combinations of failed and successful iterations among the first n – 1 iterations.

modeled as

a-within-consecutive-b-out-of-c:F system

- consists of c (c ≥ a) linearly ordered components,
- fails iff at least a (a ≤ b) components fail among any b consecutive components.

Sfakianakis et al. (1992)

$$P(C2) >= R_{abc}(k - m + 1,\ k,\ n - 1)$$

Lower-bounding dPDF (3/3)

$$P(C1) = \binom{k-1}{k-m} F^{(k-m+1)}(1-F)^{m-1}$$

$$P(C2) >= R_{abc}(k-m+1,\ k,\ n-1)$$

$$g(n) \geq g_{LB}(n) = \binom{k-1}{k-m} F^{(k-m+1)}(1-F)^{m-1} R_{abc}(k-m+1,\ k,\ n-1)$$

Given F, lower-bound the mean time to failure (MTTF)

Failure = Violation of the (m,k) constraint:

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

Outline

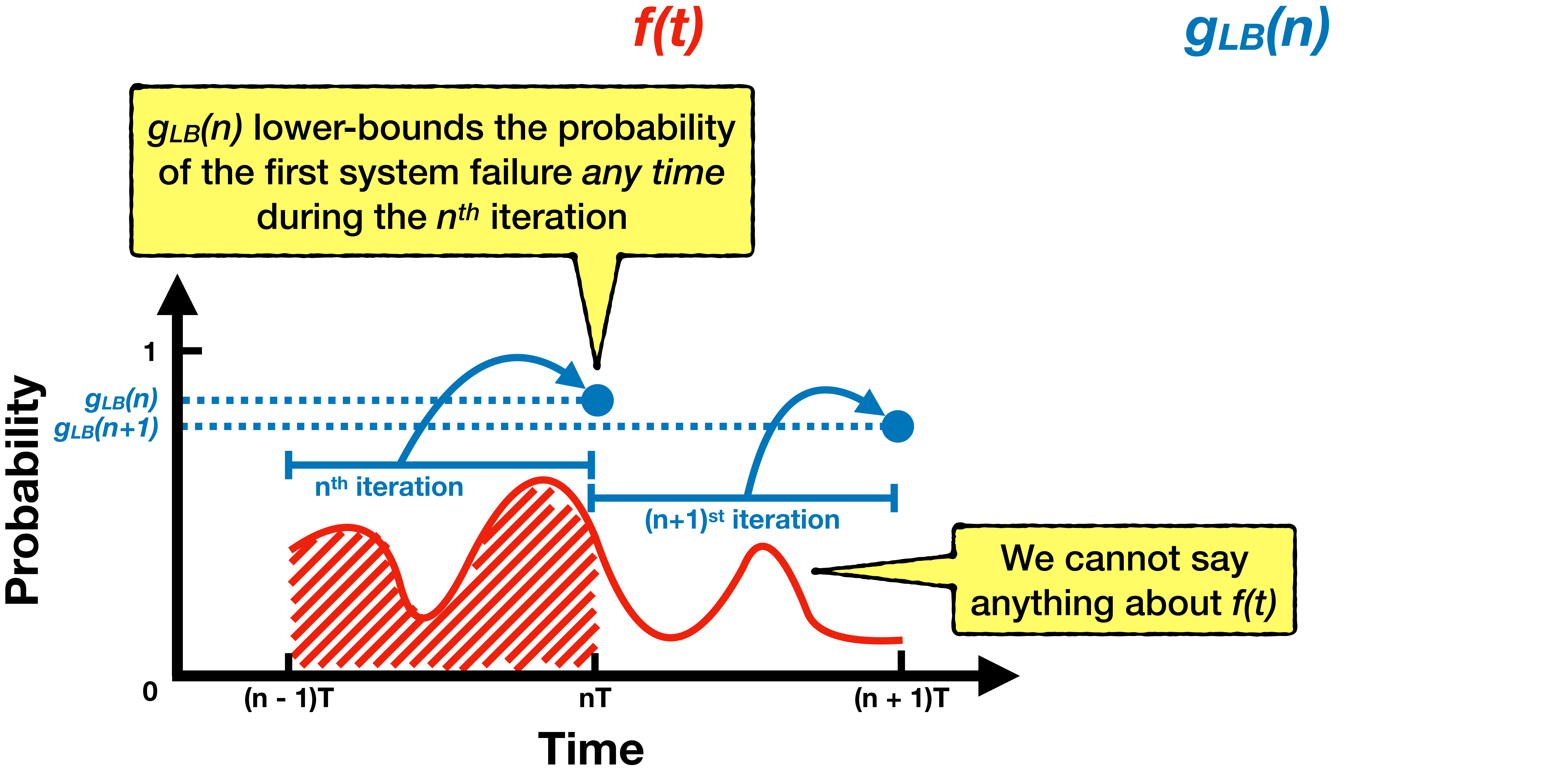
1. Discrete probability density function (dPDF)
   g(n) = P(first (m,k) violation in the n^{th} iteration)

2. Probability density function (PDF)
   f(t) = P(first (m,k) violation at time t)

3. Mean time to failure (MTTF)
   MTTF = E [system lifetime] = $\int_0^\infty t f(t)\, dt$

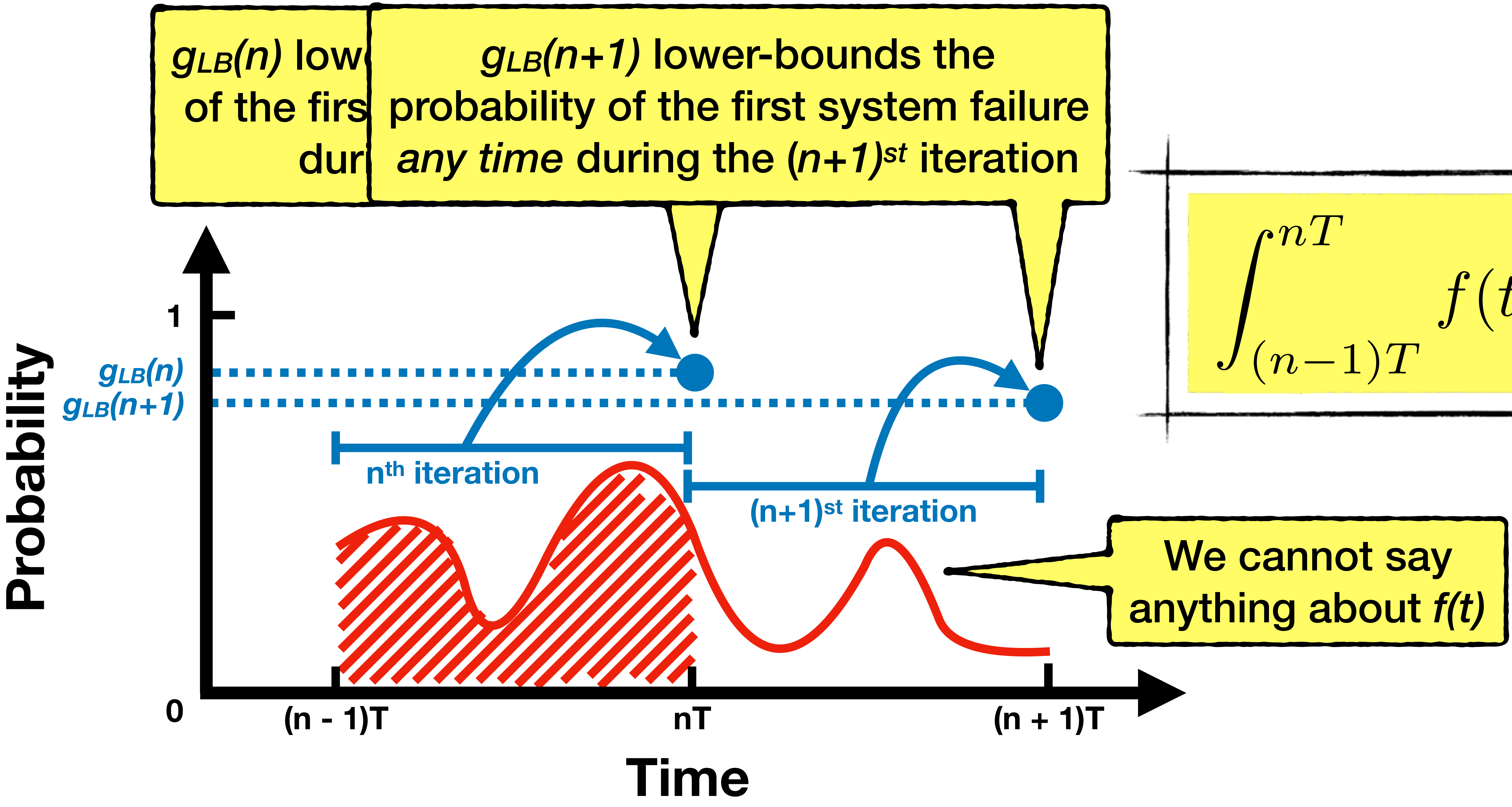
4. Evaluation

Lower-bounding PDF using dPDF lower bound



Lower-bounding PDF using dPDF lower bound

f(t) — *$g_{LB}(n)$*



$$\int_{(n-1)T}^{nT} f(t) \geq g_{LB}(n)$$

Given F, lower-bound the mean time to failure (MTTF)

Failure = Violation of the (m,k) constraint:

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

Outline

1 Discrete probability density function (dPDF)

g(n) = P(first (m,k) violation in the n^th^ iteration)

2 Probability density function (PDF)

f(t) = P(first (m,k) violation at time t)

3 Mean time to failure (MTTF)

MTTF = E [system lifetime] = $\int_0^{\infty} t f(t)\, dt$

4 Evaluation

Challenges

$$g(n) \geq g_{LB}(n) = \binom{k-1}{k-m} F^{(k-m+1)}(1-F)^{m-1} R_{abc}(k-m+1,\ k,\ n-1)$$

Problem

- Complex definition
- Multiple sub-cases
- Recursive expressions

$$\int_{(n-1)T}^{nT} f(t) \geq g_{LB}(n)$$

$$MTTF = \int_0^\infty t f(t)\, dt$$

Challenges

#	Case	Definition	Type	Source
1	$a = 0$	$R_1(a,b,c) = 0$	Exact	–
2	$a = 1$	$R_2(a,b,c) = P_S^c$	Exact	–
3	$a = 2 \wedge c \leq 4b$	$R_3(a,b,c) = \sum_{i=0}^{\lfloor \frac{c+b-1}{b} \rfloor} \binom{c-(i-1)(b-1)}{i} P_F^i P_S^{c-i}$	Exact	[12, §11.4.1] (Eqs. 11.9 and 11.10)
4	$a = 2 \wedge c > 4b$	$R_4(a,b,c) = R_3(a,b,b+t-1)(R_3(a,b,b+3))^u$ where $t = (c-b+1) \bmod 4$ and $u = \lfloor \frac{c-b+1}{4} \rfloor$	LB	[12, §11.4.1] (Eq. 11.16)
5	$a > 2 \wedge c \leq 2b \wedge a = b$	$R_5(a,b,c) = \begin{cases} 1 & 0 \leq c < a \\ 1 - P_F^a - (c-k)P_F^a P_S & a \leq c \leq 2a \end{cases}$	Exact	[12, §9.1.1] (Eqs. 9.2, 9.9, and 9.20)
6	$a > 2 \wedge c \leq 2b \wedge a \neq b \wedge c \leq b$	$R_6(a,b,c) = \sum_{i=c-a+1}^{c} \binom{c}{i} P_S^i P_F^{c-i}$	Exact	[12, §7.1.1] (Eq. 7.2)
7	$a > 2 \wedge c \leq 2b \wedge a \neq b \wedge c > b$	$R_7(a,b,c) = \sum_{i=0}^{a-1} \binom{b-s}{i} P_F^i P_S^{b-s-i} M(a',s,2s)$ where $s = c-b$ and $a' = a-i$, and $M(a',s,2s) = \begin{cases} 1 & a' > s \\ R_2(a',s,2s) & a' = 1 \\ R_3(a',s,2s) & a' = 2 \\ R_5(a',s,2s) & a' > 2 \wedge a' = s \\ R_7(a',s,2s) & a' > 2 \wedge a' \neq s \end{cases}$	Exact	[12, §11.4.1] (Eq. 11.14)
8	$a > 2 \wedge c > 2b$	$R_8(a,b,c) = R_\phi(a,b,b+t-1)(R_\phi(a,b,b+3))^u$ where $t = (c-b+1) \bmod 4$ and $u = \lfloor \frac{c-b+1}{4} \rfloor$, and $R_\phi(a,b,c) = \begin{cases} R_5(a,b,c) & a = b \\ R_6(a,b,c) & a \neq b \wedge a \leq b \\ R_7(a,b,c) & a \neq b \wedge a > b \end{cases}$	LB	[12, §11.4.1] (Eq. 11.16)

TABLE I. **Type** indicates whether the reliability definition for that respective case is an exact value or a lower bound.

$$R_{abc}(k - m + 1,\ k,\ n - 1)$$

Problem

- Complex definition
- Multiple sub-cases
- Recursive expressions

Symbolic integration not an option!

Numeric, but sound, method to lower-bound the MTTF

$$g(n) \geq \underbrace{g_{LB}(n)} = \binom{k-1}{k-m} F^{(k-m+1)} (1-F)^{m-1} R_{abc}(k-m+1,\ k,\ n-1)$$

Computing $g_{LB}(n)$ for a given < *m, k, n, F* > is easy

- *m, k, F* are constants for a given system

But what about *n*?

- n varies from 0 to ∞

$$\int_{(n-1)T}^{nT} f(t) \geq g_{LB}(n)$$

$$MTTF = \int_0^{\infty} t f(t)\, dt$$

Compute $g_{LB}(n)$ at L + 1 distinct points $d_0, d_1, \ldots, d_L$

$g_{LB}(d_0)$

$g_{LB}(d_1)$

$g_{LB}(d_2)$

⋮

$g_{LB}(d_{L-1})$

$g_{LB}(d_L)$

Paper

$$MTTF = \int_0^{\infty} t \times f(t)\,dt$$

{splitting $(0, \infty)$ into a finite number of subintervals $(0, d_0T]$, $(d_0T, d_1T]$, …, $(d_{D-1}T, d_DT]$, and (d_DT, ∞); and dropping the integrals for subintervals $(0, d_0T]$ and (d_DT, ∞) since we are interested in lower-bounding the MTTF}

$$\geq \sum_{i=0}^{D-1} \int_{d_iT}^{d_{i+1}T} t \times f(t)\,dt$$

{since for all $t \in (d_iT, d_{i+1}T]$, $t \geq d_iT$}

$$\geq \sum_{i=0}^{D-1} \left(d_iT \times \int_{d_iT}^{d_{i+1}T} f(t)\,dt \right)$$

{splitting each subinterval $(d_iT, d_{i+1}T]$ into multiple subintervals $(d_iT, (d_i+1)T]$, $((d_i+1)T, (d_i+2)T]$, …, $((d_{i+1}-1)T, (d_{i+1})T]$, each of length T}

$$= \sum_{i=0}^{D-1} \left(d_iT \times \left(\sum_{j=0}^{d_{i+1}-d_i-1} \int_{(d_i+j)T}^{(d_i+j+1)T} f(t)\,dt \right) \right)$$

{since $\int_{(d_i+j)T}^{(d_i+j+1)T} f(t)\,dt \geq g_{LB}(d_i+j+1)$ (from Eq. 2)}

$$\geq \sum_{i=0}^{D-1} \left(d_iT \times \left(\sum_{j=0}^{d_{i+1}-d_i-1} g_{LB}(d_i+j+1) \right) \right)$$

{since $g_{LB}(n)$ is decreasing with increasing n, for each integer j in the interval $[0, d_{i+1}-d_i-1]$, $g_{LB}(d_i+j+1) \geq g_{LB}(d_i + d_{i+1} - d_i - 1 + 1) = g_{LB}(d_{i+1})$}

$$\geq \sum_{i=0}^{D-1} \left(d_iT \times \left(\sum_{j=0}^{d_{i+1}-d_i-1} g_{LB}(d_{i+1}) \right) \right)$$

{simplifying the innermost summation}

$$= \sum_{i=0}^{D-1} \left(d_iT \times g_{LB}(d_{i+1}) \times (d_{i+1} - d_i) \right) \quad \square$$

starting with

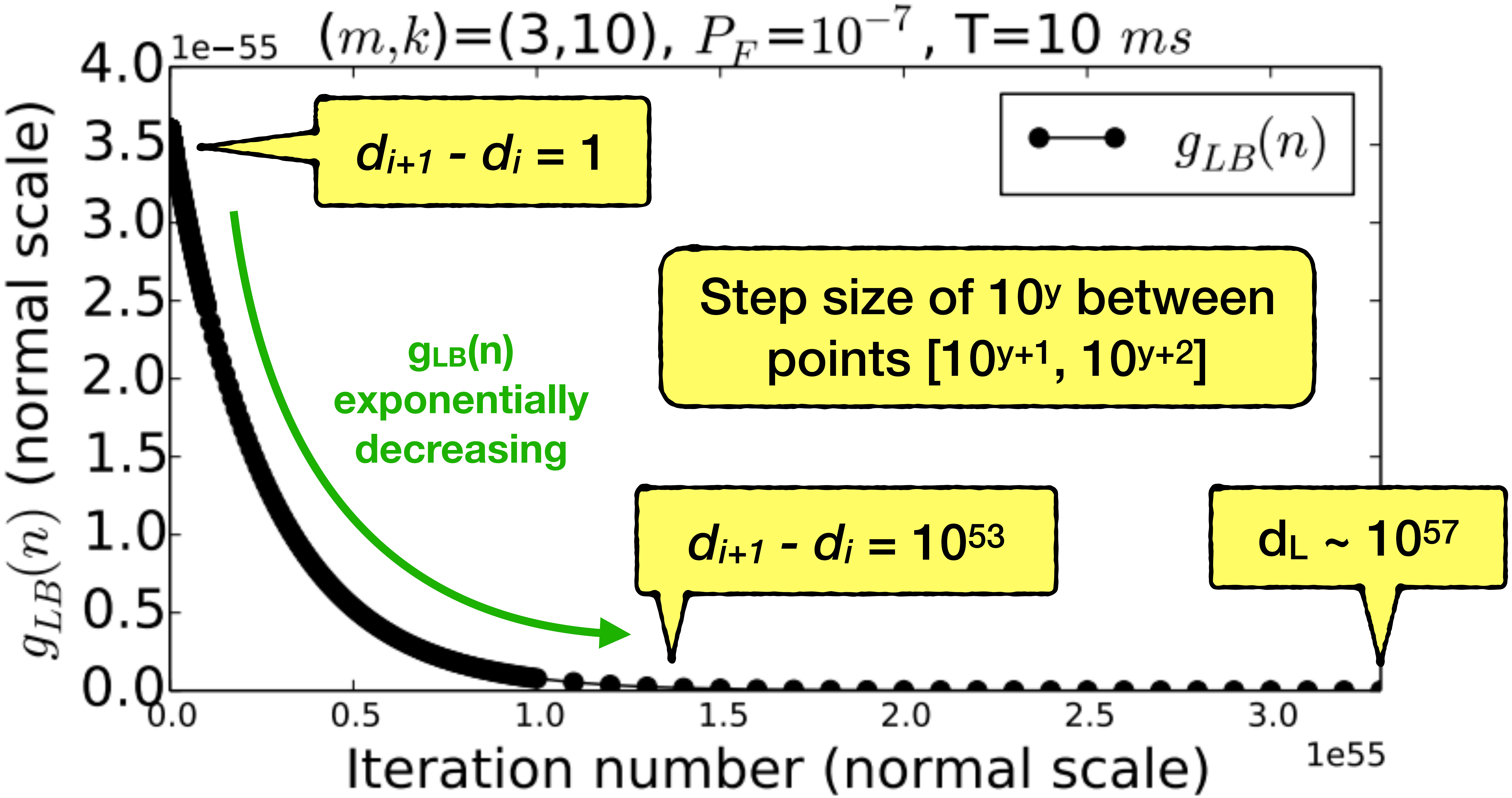
$$MTTF = \int_0^{\infty} t f(t)\,dt$$

using the relation between PDF and dPDF

$$\int_{(n-1)T}^{nT} f(t) \geq g_{LB}(n)$$

$$MTTF \geq \sum_{i=0}^{L-1} \left(d_i \cdot g_{LB}(d_{i+1}) \cdot (d_{i+1} - d_i) \cdot T \right)$$

Choosing points d_0, d_1, ..., d_L



Given F, lower-bound the mean time to failure (MTTF)

Failure = Violation of the (m,k) constraint:

At least ***m*** iterations, out of any ***k*** consecutive loop iterations must be correct

Outline

1 Discrete probability density function (dPDF)

g(n) = P(first (m,k) violation in the n^{th} iteration)

2 Probability density function (PDF)

f(t) = P(first (m,k) violation at time t)

3 Mean time to failure (MTTF)

MTTF = E [system lifetime] = $\int_0^\infty t f(t)\, dt$

4 Evaluation

Approximating MTTF using simulation

Biased-coin toss experiment

Tails with probability *F*
- system iteration is incorrect

Heads with probability *1 - F*
- system iteration is correct

Each trial

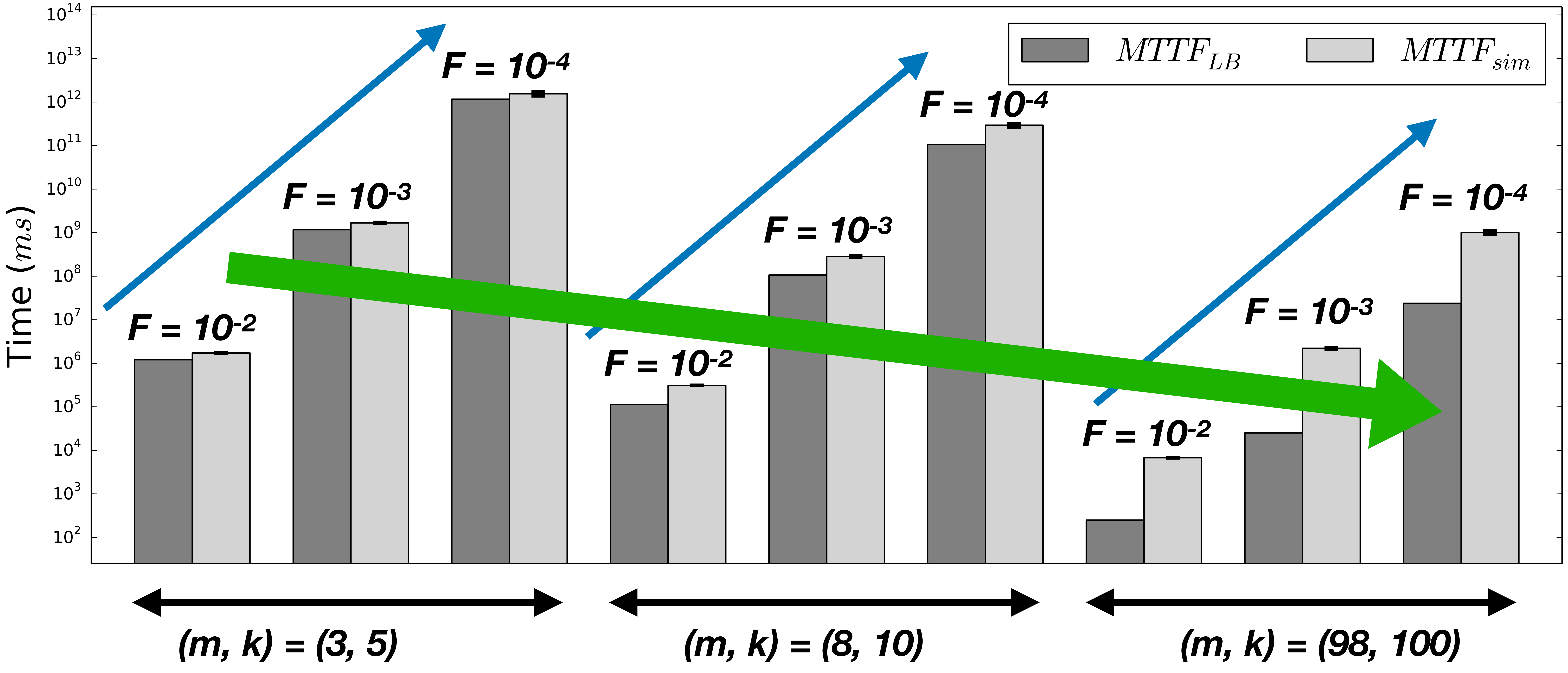
Repeat coin toss until the (m,k) constraint is violated

$MTTF_{sim}$ = Average tosses per trial x control period

Comparing $MTTF_{LB}$ and $MTTF_{sim}$

MTTF increases when *F* decreased from 10^{-2} to 10^{-4}

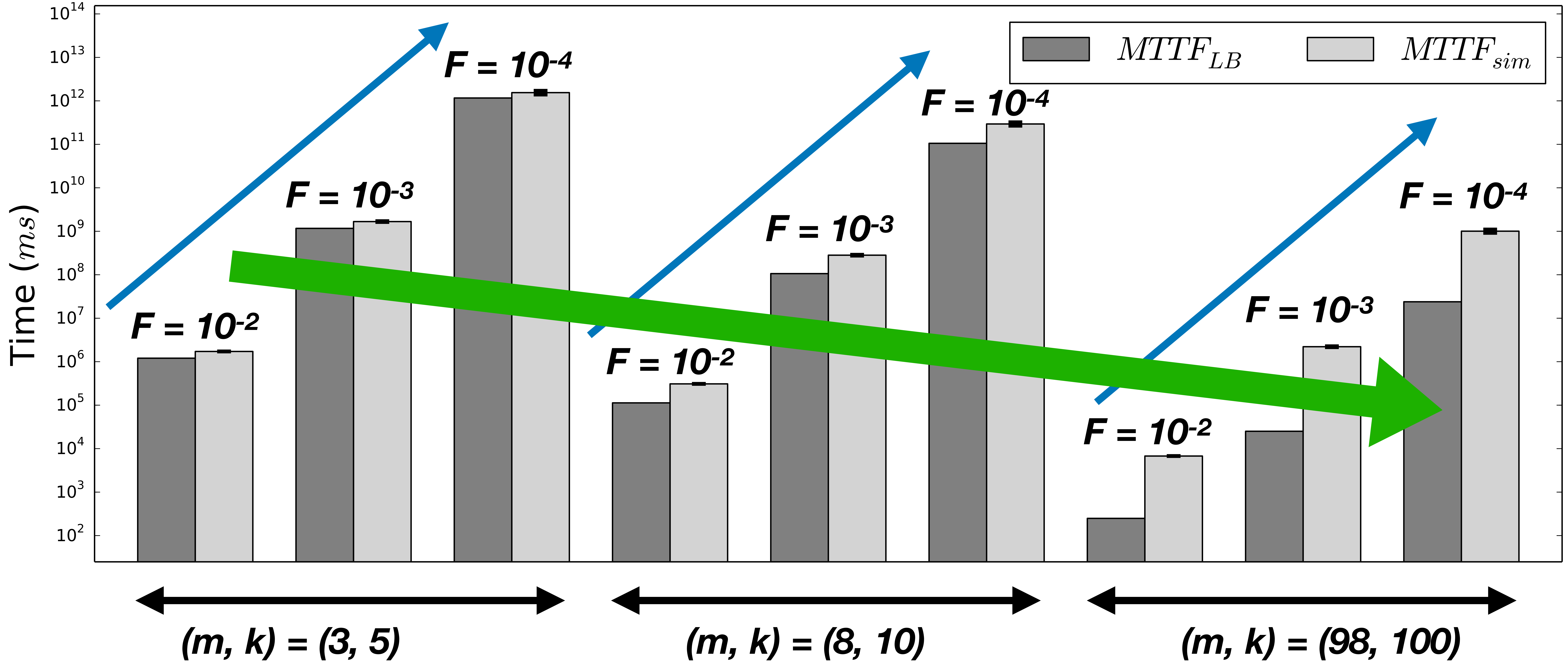
MTTF decreases when *m/k* increased from 3/5 to 98/100



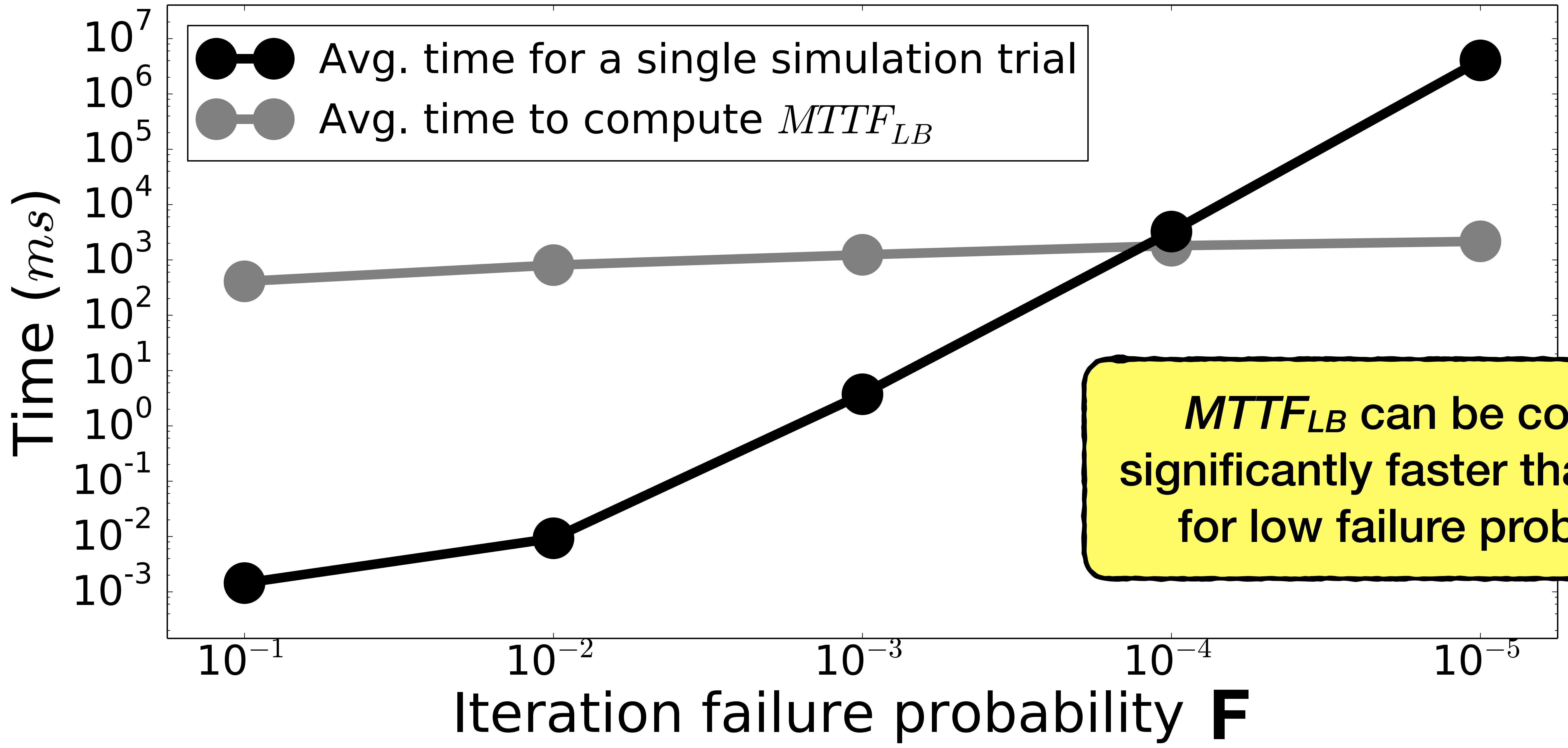
Comparing $MTTF_{LB}$ and $MTTF_{sim}$

$MTTF_{LB}$ is always less than $MTTF_{sim}$

In all cases, $MTTF_{LB}$ and $MTTF_{sim}$ are roughly of the same orders of magnitude

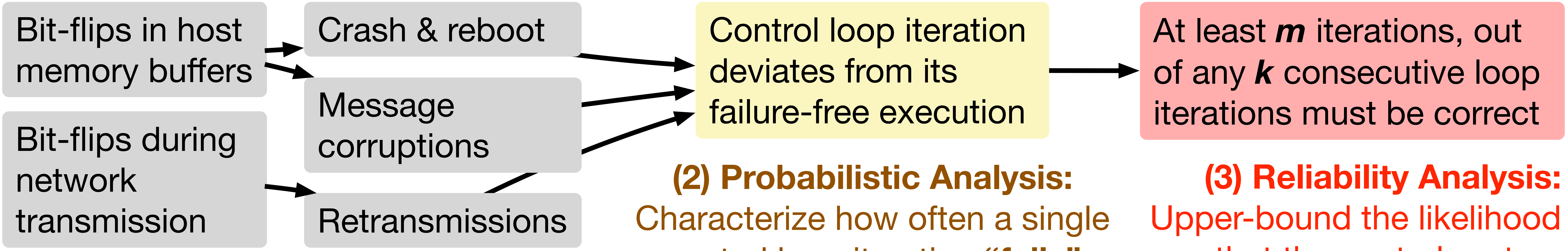


Comparing time to compute $MTTF_{LB}$ and $MTTF_{sim}$



$MTTF_{LB}$ can be computed significantly faster than *$MTTF_{sim}$* for low failure probabilities

Summary



(1) Fault Modeling: Transient faults modeled using **Poisson** distribution, empirically-derived **peak EMI** rates

(2) Probabilistic Analysis: Characterize how often a single control loop iteration **"fails"**

(3) Reliability Analysis: Upper-bound the likelihood that the control system **"fails beyond recovery"**

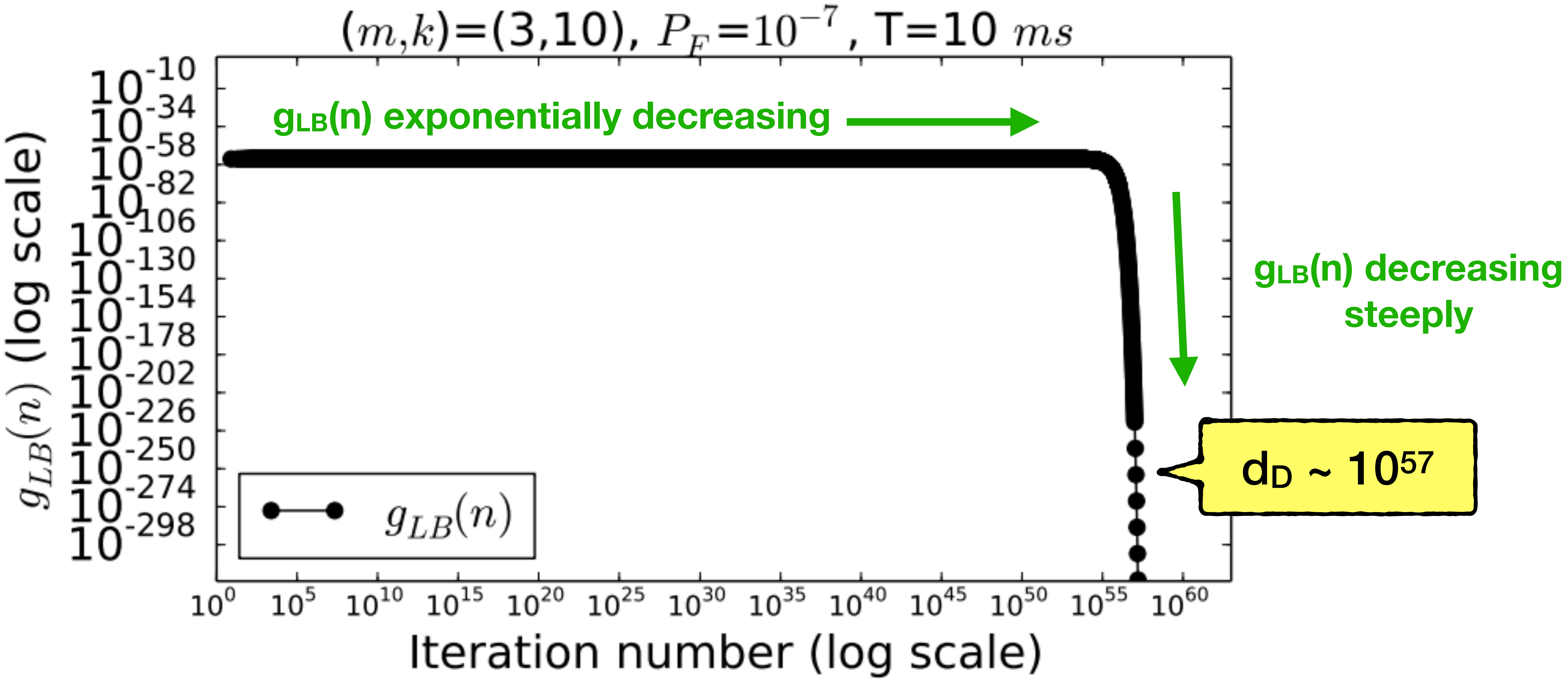
Given a bound *F* on the iteration failure probability, also satisfying the IID property

→

Safe lower bound on the system MTTF for systems with *(m, k)* constraints

Thank you. Questions?

Backup



(m,k)=(3,10), P_F=10^-7, T=10 ms
g_LB(n) exponentially decreasing
g_LB(n) decreasing steeply
d_D ~ 10^57
g_LB(n)
g_LB(n) (log scale)
10^-10
10^-34
10^-58
10^-82
10^-106
10^-130
10^-154
10^-178
10^-202
10^-226
10^-250
10^-274
10^-298
10^0
10^5
10^10
10^15
10^20
10^25
10^30
10^35
10^40
10^45
10^50
10^55
10^60
Iteration number (log scale)