Lower-Bounding the MTTF for Systems with (m, k) Constraints and IID Iteration Failure Probabilities

Arpan Gujarati, Mitra Nasri, and Björn B. Brandenburg
Max Planck Institute for Software Systems (MPI-SWS), Germany
{arpanbg, mitra, bbb}@mpi-sws.org

Technical Report MPI-SWS-2018-004r*
July 2018

***Abstract*—We derive a sound lower bound on the *mean time to failure* of periodic systems with (m, k) constraints. We assume that upper bounds on the failure probabilities of each system iteration, *e.g.*, a job or a runtime activation of a periodic task, or a single actuation cycle of a control loop, are known and that they satisfy the IID assumption. Our analysis leverages prior work on the well-studied *a-within-consecutive-b-out-of-c:F* system model.**

I. Introduction

For safety certification, the reliability of a safety-critical system must be carefully analyzed before deployment. Typically, this is done using generic analyses such as *fault tree analysis* (FTA) [18] and *failure mode and effects analysis* (FMEA) [19], or domain-specific analyses (*e.g.* [5, 16]). The analyzed reliability is reported using metrics such as the *mean time to failure* (MTTF) or the *failures-in-time* (FIT) [20], or sometimes simply using a failure probability.

Many periodic safety-critical systems are subject to (m, k) constraints, *i.e.*, at least m iterations out of any k consecutive iterations must be correct [10]. For example, many real-time systems can tolerate a few deadline misses [11] and well-designed, robust control applications remain functional despite a few missed or incorrect actuations [4], thanks to the underlying physics. However, accurate and sound reliability analysis of systems with (m, k) constraints is still an open problem.

Prior works focus on the reliability analysis of individual iterations, *e.g.*, analyzing the probability of a deadline miss or a faulty message transmission in any iteration, as in [3, 8, 16], and then extrapolate overall reliability guarantees for the system, *e.g.*, by analyzing the probability of *no* deadline misses or *no* faulty message transmissions. For systems with (m, k) constraints, this zero-tolerance hard real-time approach towards reliability analysis results in excessively pessimistic reliability bounds, and consequently in cost-inefficient designs that under-utilize system resources.

In this work, we propose a new reliability analysis for systems with (m, k) constraints. We assume that (an upper bound on) the failure probability for each iteration is known in advance and that these iteration failure probabilities satisfy the *IID assumption* (*i.e.*, they are identical for each iteration and are independent of other failed iterations). For instance, this assumption is satisfied by Broster et al.'s analysis [3] of the probability of a timely transmission of a Controller Area Network (CAN) message, or our prior work [8] on the reliability analysis of replicated CAN messages.

We then leverage existing results on the reliability analysis of the well-studied *a-within-consecutive-b-out-of-c:F* system model [12] to derive the probability that the system violates its (m, k) constraint for the first time during the n^{th} iteration. Finally, using these probabilities, we characterize the system reliability in terms of a lower bound on its MTTF.

This work is part of an ongoing project on reliability analysis of CAN-based *networked control systems* (NCS) with replicated tasks that are characterized using (m, k) constraints. We are currently developing an analysis to derive IID failure probabilities for each iteration of a control loop in the NCS, which, together with the analysis presented in this paper, will help quantify the overall reliability of the NCS.

II. System Model

Let P_F (for **F**ailure) denote an upper bound on the probability that a single iteration of the system fails, and let $P_S = 1 - P_F$ (for **S**uccess). We assume that $0 < P_F < 1$ and that P_F satisfies the IID assumption. Since reliability analyses, such as the ones in [3, 8], often analyze the worst-case scenario for *any* iteration, the resulting iteration failure probabilities satisfy this assumption.

Let S denote the system being analyzed and T denote its activation period. S *fails* as soon as it violates the (m, k) constraint. That is, it fails during the n^{th} iteration if the n^{th} iteration fails and it is the $(k - m + 1)^{\text{th}}$ failed iteration in the last k iterations (thus violating the (m, k) constraint), and if the (m, k) constraint has not been violated before. This implies that S cannot fail during the first $k - m$ iterations.

The MTTF of a system is defined as its *expected lifetime*. That is, for a system S with an (m, k) constraint, MTTF is the average time that it takes for S to violate its (m, k) constraint. It can be computed using the well-known definition $MTTF = \int_0^\infty t \times f(t)\, dt$ [12, §2.2], where $f(t)$ denotes the *probability density function* (*p.d.f.*) of S, *i.e.* the probability that S violates its (m, k) constraint for the first time at time instant t. The

*This report refines and supersedes the original version published in April 2018 as Technical Report MPI-SWS-2018-004.

objective of this paper is to derive a lower bound on the MTTF of system S, given its iteration failure probability P_F.

III. Overview

The proposed analysis consists of four steps. In Step 1, we formulate the probability that S violates its (m, k) constraint for the first time in its n^{th} iteration. In Step 2, we define a lower bound on this probability, since obtaining an exact value is computationally hard. In Step 3, we lower-bound the *p.d.f.* of S, which is required for computing its MTTF. Finally, in Step 4, we derive a lower bound on the MTTF using the lower bound on the *p.d.f.* Steps 1-4 are explained in detail below.

Step 1. S violates its (m, k) constraint for the first time in its n^{th} iteration if the following conditions hold:

E_1: The n^{th} iteration must fail.

E_2: Exactly $k-m$ iterations must fail out of the $k-1$ iterations between the $(n-k+1)^{\text{th}}$ and the $(n-1)^{\text{th}}$ iteration.

E_3: Fewer than $k-m+1$ iterations fail out of any k consecutive iterations, among the first $n-1$ iterations.

Thus, given E_1, E_2, and E_3, the probability that S violates its (m, k) constraint for the first time in its n^{th} iteration is lower-bounded by $P(E_1) \times P(E_2) \times P(E_3)$.

Step 2. From §II, $P(E_1) = P_F$. Summing over all possible combinations of $k-m$ iteration failures in $k-1$ consecutive iterations, $P(E_2) = \binom{k-1}{k-m} P_F^{(k-m)} P_S^{(m-1)}$. But obtaining the exact value of $P(E_3)$ is computationally challenging, since it requires evaluating all possible combinations of failed and successful iterations among the first $n-1$ iterations.

Thus, we approximate $P(E_3)$ using the well-studied a-within-consecutive-b-out-of-c:F system [12, §11.4], which consists of c ($c \geq a$) linearly ordered components, and which fails iff at least a ($a \leq b$) components fail among any b consecutive components. That is, in terms of the (m, k) model, an a-within-consecutive-b-out-of-c:F system fails if it violates the $(b-a+1, b)$ constraint. We refer to this system model as an a/Con/b/c:F system, for brevity. We model E_3 as an a/Con/b/c:F system where $a = k-m+1$, $b = k$, and $c = n-1$, and lower-bound $P(E_3)$ using a reliability lower bound $R_{LB}(a, b, c)$ of this system, which we will introduce in §IV.

From the above definitions of $P(E_1)$, $P(E_3)$, $P(E_3)$, if $n > k-m$, a lower bound on the probability that S violates its (m, k) constraint for the first time during its n^{th} iteration is:

$$g_{LB}(n) = \binom{k-1}{k-m} P_F^{(k-m+1)} P_S^{(m-1)} \times R_{LB}(k-m+1,\, k,\, n-1). \quad (1)$$

Step 3. Recall from §II that T denotes the period of system S. Accordingly, any time t such that $(n-1)T < t \leq nT$ corresponds to the execution of the n^{th} iteration of S. Thus, the sum of the *p.d.f.* of system S at all time instants in $((n-1)T,\, nT]$ is lower bounded by $g_{LB}(n)$, *i.e.*,

$$\int_{(n-1)T}^{nT} f(t) \geq g_{LB}(n). \quad (2)$$

In addition, $f(t) = 0$, *i.e.*, the system is reliable, for all $t \leq (k-m)T$ since by definition of the (m, k) constraint, the system can fail only after $k-m$ iterations.

Step 4. A lower bound on the MTTF is derived using the expression $MTTF = \int_0^\infty t \times f(t)\, dt$ and Eq. 2. However, since $g_{LB}(n)$ in Eq. 2 is defined in terms of $R_{LB}(k-m+1, k, n-1)$, a recursive expression with complex definitions of its subproblems (see §IV), symbolic integration to lower bound the MTTF is infeasible, even with tools such as Mathematica [1].

Instead, we propose a numeric, but sound approach to lower-bound the MTTF that relies on computing the value of $g_{LB}(n)$ at finitely many data points (see §V).

IV. The a/Con/b/c:F System Model

We assume that the system consists of IID components.[1] We first define a lower bound on the reliability of an *a/Con/b/c:F* system, *i.e.*, a lower bound on the probability that the system does not fail, using prior results and then prove that this lower bound decreases with increasing c if certain conditions hold.

A. Reliability of an a/Con/b/c:F system

Let $R(a, b, c)$ denote the exact reliability of an a/Con/b/c:F system. A brute-force approach to compute $R(a, b, c)$ requires enumerating all combinations of failed/not-failed components, selecting the combinations for which the system does not fail, and then adding the event probabilities for these reliable combinations. However, since the number of combinations that need to be checked are exponential in c, the brute-force approach is infeasible, particularly since c can easily exceed 10^{50} (see §VI for details).

We instead use the results of Sfakianakis et al. [17] to derive a lower bound on $R(a, b, c)$, denoted $R_{LB}(a, b, c)$, for large values of c. Sfakianakis et al.'s analysis breaks the problem into smaller subproblems for which exact analyses are available. Their analysis, as well as the exact analyses for different types of subproblems, are explained in detail in [12].

Table I summarizes the relevant results in [12] for different values of a, b, and c. Cases 1 and 2 are trivial: if $a = 0$, the system is always unreliable, and if $a = 1$, the system is reliable only if none of the c components fail. Cases 3, 5, 6, and 7 correspond to special cases where c is small (less than or equal to either $2b$ or $4b$) and for which exact reliabilities can be computed. Cases 4 and 8 correspond to large, unbounded values of c and are resolved using Sfakianakis et al.'s recursive analysis. A generic lower bound $R_{LB}(a, b, c)$ is defined by combining all of these cases.

B. $R_{LB}(a, b, c)$ decreases with increasing c

The MTTF analysis in §V depends on the property that $R_{LB}(a, b, c)$ *decreases with increasing* c. This property trivially holds for cases $a = 0$ and $a = 1$, as seen from the definitions of $R_1(a, b, c)$ and $R_2(a, b, c)$ in Table I. However,

[1] We use the terms *iteration* and *component* interchangeably. We use the term *component* in this section since it is consistent with the terminology used in the existing literature on the a/Con/b/c:F model.

#	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 $R_\phi(a,b,c) = \begin{cases} R_5(a,b,c) & a = b \\ R_6(a,b,c) & a \neq b \wedge c \leq b \\ R_7(a,b,c) & a \neq b \wedge c > b \end{cases}$	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.

proving the property for cases $a > 2$ and $a = 2$ is non-trivial and discussed explicitly in Lemmas 1 and 2, respectively.

Notice that case $a > 2$ corresponds to multiple cases (5-8) in Table I. In fact, because of the recursive definitions for some of these cases, case $a > 2$ actually depends on the remaining cases as well, which makes it hard to prove that $R_{LB}(a,b,c)$ decreases with increasing c. Instead, we prove a weaker property: we show that *if* $R_{LB}(a,b,c)$ decreases with increasing c for small values of c (*i.e.*, for $c \leq 2b$), *then* $R_{LB}(a,b,c)$ also decreases with increasing c for larger values of c (*i.e.*, for $c > 2b$). Since b is typically relatively small, *i.e.*, $b = k$ (recall Step 2 from §III), the *if* condition can be easily checked for specific values of a, b, c and p through exhaustive enumeration.

Lemma 1. *For $c \geq a$ and $a > 2$, if $R_{LB}(a,b,c)$ is monotonically decreasing for $c \in \{a, \ldots, 2b+1\}$, then $R_{LB}(a,b,c)$ is also monotonically decreasing for $c \geq 2b+1$, i.e.,*

$$\begin{aligned} &\textit{if} && \forall c \leq 2b: \; R_{LB}(a,b,c) \geq R_{LB}(a,b,c+1), \\ &\textit{then} && \forall c > 2b: \; R_{LB}(a,b,c) \geq R_{LB}(a,b,c+1). \end{aligned} \quad (3)$$

Proof. In the following, given the *if* condition, we prove the *then* condition separately for cases $(c-b+1) \bmod 4 = 3$ and $(c-b+1) \bmod 4 < 3$, respectively. Note that for both the cases, $c > 2b$ (from Eq. 3).

Case 1 [$(c-b+1) \bmod 4 = 3$].

$$\frac{R_{LB}(a,b,c)}{R_{LB}(a,b,c+1)}$$

{since $a > 2$ and $c > 2b$, both terms $R_{LB}(a,b,c)$ and $R_{LB}(a,b,c+1)$ are resolved using case 8 in Table I; thus, from $R_8(a,b,c)$'s definition, and letting $x = c-b+1$}

$$= \frac{R_\phi(a,b,b+(x \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_\phi(a,b,b+((x+1) \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 = 3$ implies $(x+1) \bmod 4 = 0$}

$$= \frac{R_\phi(a,b,b+2)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_\phi(a,b,b-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 = 3$ implies $\lfloor \frac{x+1}{4} \rfloor = \lfloor \frac{x}{4} \rfloor + 1$}

$$= \frac{R_\phi(a,b,b+2)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_\phi(a,b,b-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor + 1}}$$

{dividing numerator and denominator by $(R_\phi(a,b,b-1))^{\lfloor \frac{x}{4} \rfloor}$}

$$= \frac{R_\phi(a,b,b+2)}{R_\phi(a,b,b+3)R(a,b,b+3)}$$

{since $R_\phi(a,b,b-1) \leq 1$ (being a probability), and letting $c' = b+2$}

$$\geq \frac{R_\phi(a,b,c')}{R_\phi(a,b,c'+1)}$$

{recall from §III that $a \leq b$; hence, $2 < a \implies 2 < b \implies 2+b < 2b \implies c' \leq 2b$}

{since $c' \leq 2b$, $R_{LB}(a,b,c') \geq R_{LB}(a,b,c'+1)$ from the *if* condition in Eq. 3; this can be further simplified using the definitions of $R_{LB}(a,b,c')$ and $R_{LB}(a,b,c'+1)$ from Cases 5-8 in Table I as follows: $R_\phi(a,b,c') \geq R_\phi(a,b,c'+1)$}

$\geq 1.$

Case 2 [$(c-b+1) \bmod 4 < 3$].

$$\frac{R_{LB}(a,b,c)}{R_{LB}(a,b,c+1)}$$

{since $a > 2$ and $c > 2b$, both terms $R_{LB}(a,b,c)$ and $R_{LB}(a,b,c+1)$ are resolved using case 8 in Table I; thus, from $R_8(a,b,c)$'s definition, and letting $x = c-b+1$}

$$= \frac{R_\phi(a,b,b+(x \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_\phi(a,b,b+((x+1) \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 < 3$ implies $\lfloor \frac{x+1}{4} \rfloor = \lfloor \frac{x}{4} \rfloor$}

$$= \frac{R_\phi(a,b,b+(x \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_\phi(a,b,b+((x+1) \bmod 4)-1)(R_\phi(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}$$

{dividing numerator and denominator by $(R(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}$}

$$= \frac{R_\phi(a,b,b+(x \bmod 4)-1)}{R_\phi(a,b,b+((x+1) \bmod 4)-1)}$$

{since $x \bmod 4 < 3$ implies $(x+1) \bmod 4 = 1 + x \bmod 4$}

$$= \frac{R_\phi(a,b,b+(x \bmod 4)-1)}{R_\phi(a,b,b+(x \bmod 4))}$$

{letting $c' = b+(x \bmod 4)-1$}

$$= \frac{R_\phi(a,b,c')}{R_\phi(a,b,c'+1)}$$

{**(i)** $x \bmod 4 < 3 \implies b+(x \bmod 4)-1 < b+2 \implies c' < b+2$; **(ii)** also recall from §III that $a \leq b$, and hence, $2 < a \implies 2 < b \implies 2+b < 2b$; from (i) and (ii), $c' < 2b$}

{since $c' \leq 2b$, $R_{LB}(a,b,c') \geq R_{LB}(a,b,c'+1)$ from the *if* condition in Eq. 3; this can be further simplified using the definitions of $R_{LB}(a,b,c')$ and $R_{LB}(a,b,c'+1)$ from Cases 5-8 in Table I as follows: $R_\phi(a,b,c') \geq R_\phi(a,b,c'+1)$}

$\geq 1.$ $\square$

For case $a = 2$, we once again prove a weaker property similar to that for case $a > 2$: we show that *if* $R_{LB}(a,b,c)$ decreases with increasing c for small values of c (*i.e.*, for $c \leq 4b$), *then* $R_{LB}(a,b,c)$ also decreases with increasing c for larger values of c (*i.e.*, for $c > 4b$).

Lemma 2. *For $c \geq a$ and $a = 2$, if $R_{LB}(a,b,c)$ is monotonically decreasing for $c \in \{a, \ldots, 4b+1\}$, then $R_{LB}(a,b,c)$ is also monotonically decreasing for $c \geq 4b+1$, i.e.,*

$$\begin{aligned} &\textit{if} && \forall c \leq 4b: \; R_{LB}(a,b,c) \geq R_{LB}(a,b,c+1), \\ &\textit{then} && \forall c > 4b: \; R_{LB}(a,b,c) \geq R_{LB}(a,b,c+1). \end{aligned} \quad (4)$$

Proof. In the following, given the *if* condition, we prove the *then* condition separately for cases $(c-b+1) \bmod 4 = 3$ and $(c-b+1) \bmod 4 < 3$, respectively. Note that for both the cases, $c > 4b$ (from Eq. 4).

Case 1 [$(c-b+1) \bmod 4 = 3$].

$$\frac{R_{LB}(a,b,c)}{R_{LB}(a,b,c+1)}$$

{since $a = 2$ and $c > 4b$, both terms $R_{LB}(a,b,c)$ and $R_{LB}(a,b,c+1)$ are resolved using case 4 in Table I; thus, from $R_4(a,b,c)$'s definition, and letting $x = c-b+1$}

$$= \frac{R_3(a,b,b+(x \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_3(a,b,b+((x+1) \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 = 3$ implies $(x+1) \bmod 4 = 0$}

$$= \frac{R_3(a,b,b+2)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_3(a,b,b-1)(R_3(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 = 3$ implies $\lfloor \frac{x+1}{4} \rfloor = \lfloor \frac{x}{4} \rfloor + 1$}

$$= \frac{R_3(a,b,b+2)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_3(a,b,b-1)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor+1}}$$

{dividing numerator and denominator by $(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}$}

$$= \frac{R_3(a,b,b+2)}{R_3(a,b,b-1)R_3(a,b,b+3)}$$

{since $R_\phi(a,b,b-1) \leq 1$ (being a probability), and letting $c' = b+2$}

$$\geq \frac{R_3(a,b,c')}{R_3(a,b,c'+1)}$$

{recall from §III that $a \leq b$; hence, $2 = a \implies 2 \leq b \implies 2+b \leq 2b \implies c' \leq 2b \implies c' < 4b$}

{since $c' < 4b$, $R_{LB}(a,b,c') \geq R_{LB}(a,b,c'+1)$ from the *if* condition in Eq. 4; this can be further simplified using the definitions of $R_{LB}(a,b,c')$ and $R_{LB}(a,b,c'+1)$ from Case 3 in Table I as follows: $R_3(a,b,c') \geq R_3(a,b,c'+1)$}

$\geq 1.$ $\geq 1.$

Case 2 [$(c-b+1) \bmod 4 < 3$].

$$\frac{R_{LB}(a,b,c)}{R_{LB}(a,b,c+1)}$$

{since $a = 2$ and $c > 4b$, both terms $R_{LB}(a,b,c)$ and $R_{LB}(a,b,c+1)$ are resolved using case 4 in Table I; thus, from $R_4(a,b,c)$'s definition, and letting $x = c - b + 1$}

$$= \frac{R_3(a,b,b+(x \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_3(a,b,b+((x+1) \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x+1}{4} \rfloor}}$$

{since $x \bmod 4 < 3$ implies $\lfloor \frac{x+1}{4} \rfloor = \lfloor \frac{x}{4} \rfloor$}

$$= \frac{R_3(a,b,b+(x \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}{R_3(a,b,b+((x+1) \bmod 4)-1)(R_3(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}}$$

{dividing numerator and denominator by $(R(a,b,b+3))^{\lfloor \frac{x}{4} \rfloor}$}

$$= \frac{R_3(a,b,b+(x \bmod 4)-1)}{R_3(a,b,b+((x+1) \bmod 4)-1)}$$

{since $x \bmod 4 < 3$ implies $(x+1) \bmod 4 = 1 + x \bmod 4$}

$$= \frac{R_3(a,b,b+(x \bmod 4)-1)}{R_3(a,b,b+(x \bmod 4))}$$

{letting $c' = b + (x \bmod 4) - 1$}

$$= \frac{R_3(a,b,c')}{R_3(a,b,c'+1)}$$

{**(i)** $x \bmod 4 < 3 \implies b + (x \bmod 4) - 1 < b + 2 \implies c' < b + 2$; **(ii)** also recall from §III that $a \leq b$, and hence, $2 = a \implies 2 \leq b \implies 2 + b \leq 2b \implies 2 + b < 4b$; from (i) and (ii), $c' < 4b$ }

{since $c' \leq 4b$, $R_{LB}(a,b,c') \geq R_{LB}(a,b,c'+1)$ from the *if* condition in Eq. 4; this can be further simplified using the definitions of $R_{LB}(a,b,c')$ and $R_{LB}(a,b,c'+1)$ from Case 3 in Table I as follows: $R_3(a,b,c') \geq R_3(a,b,c'+1)$}

$\geq 1.$ $\square$

In the next section, while describing the proposed MTTF analysis, we assume that $R_{LB}(a,b,c)$ *decreases with increasing* c. When applying the proposed analysis (*e.g.*, in §VI), for every use of $R_{LB}(a,b,c)$, we check that the *if* condition in Lemma 1 holds in order to justify this assumption.

V. MTTF Analysis

Recall the definition of $g_{LB}(n)$ from §III (Eq. 1). Since $R_{LB}(a,b,c)$ decreases with increasing c and since $g_{LB}(n)$ is defined in terms of $R_{LB}(k-m+1,k,n-1)$, $g_{LB}(n)$ also decreases with increasing n.

Assume that the value of the function $g_{LB}(n)$ is known (*i.e.*, computed) at finitely many data points d_0, d_1, d_2, …, d_D, such that each $d_i \in \mathbb{N}$ and $k - m + 1 = d_0 < d_1 < d_2 < \ldots < d_D$. Using time instants d_0T, d_1T, d_2T, …, d_DT corresponding to the start time of iterations d_0, d_1, d_2, …, d_D, and the property that $g_{LB}(n)$ is decreasing with increasing n, we derive a lower bound on the MTTF as follows.

Lemma 3.

$$MTTF \geq \sum_{i=0}^{D-1} \Big(d_iT \times g_{LB}(d_{i+1}) \times (d_{i+1} - d_i) \Big) \qquad (5)$$

Proof.

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

{splitting $(0,\infty)$ into a finite number of subintervals $(0, d_0T]$, $(d_0T,\, d_1T]$, …, $(d_{D-1}T,\, d_DT]$, and $(d_DT,\, \infty)$; and dropping the integrals for subintervals $(0, d_0T]$ and $(d_DT,\, \infty)$ 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 $[0,\, d_{i+1}-d_i-1]$, $g_{LB}(d_i+j+1) \geq g_{LB}(d_i + d_{i+1} - d_i - 1 + 1) = g_{LB}(d_{i+1})$}

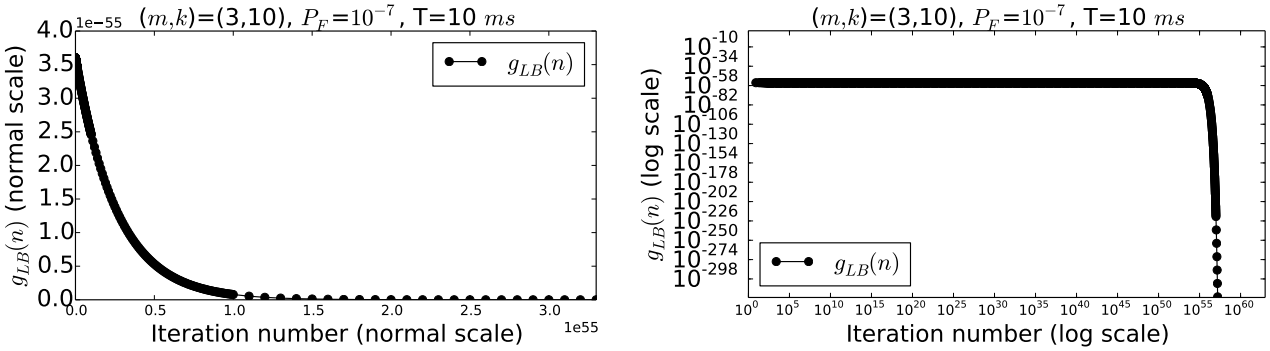
$$\geq \sum_{i=0}^{D-1} \left(d_iT \times \left(\sum_{j=0}^{d_{i+1}-d_i-1} g_{LB}(d_{i+1}) \right) \right)$$

{simplifying the innermost summation}

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

Let $MTTF_{LB}$ denote the lower bound derived in Lemma 3. If $D \ll d_D$, $MTTF_{LB}$ can be computed quickly. If the individual data points d_0, d_1, d_2, …, d_D are appropriately chosen, then the computed $MTTF_{LB}$ is sufficiently close to the exact MTTF. We revisit the choice of data poitns in §VI.

Next, we discuss how to estimate the MTTF using simulations. We use a *biased coin toss* experiment, where the biased coin comes up with heads with probability P_S, and tails with probability $P_F = 1 - P_S$. *Tails* denotes that the system iteration is incorrect, and *heads* denotes that the system iteration is correct. In each trial, the coin toss is repeated until tails is encountered $k-m+1$ times among the last k consecutive coin tosses. If Ω denotes the total number of trials and ω_i denotes the number of coin tosses during the i^{th} trial, averaging ω_i over Ω trials, *i.e.*, $\hat{\omega} = (\sum_{i=1}^{\Omega} \omega_i)/\Omega$, gives the expected number of iterations required to violate the (m,k) constraint. Using



(a) $MTTF_{LB} = 2.34 \times 10^{55}\, ms$

(b) Same as (a), but with log-scale axes

Fig. 1: **(a)** $g_{LB}(t)$ for $m = 3$, $k = 10$, and $P_F = 10^{-7}$, where $D = 5050$ and $d_D = 9.90 \times 10^{57}$. **(b)** $g_{LB}(t)$ for the same parameters, except that both the x- and y-axes are log-scale.

$\hat{\omega}$, the MTTF is estimated as $MTTF_{sim} = \hat{\omega} \times T$.

$MTTF_{sim}$ cannot be used to safely lower-bound S's reliability because it may over-approximate the reliability. However, it is a useful baseline for evaluating $MTTF_{LB}$. By comparing $MTTF_{LB}$ with $MTTF_{sim}$, we determine how much accuracy we loose by sampling D data points when deriving $MTTF_{LB}$.

VI. Evaluation

The objective of this section is twofold. First, we discuss the method used to choose the data points d_0, d_1, d_2, …, d_D. Second, we present results from a comparison of $MTTF_{LB}$ and $MTTF_{sim}$ for different values of m, k, and P_F.

A. Choosing d_0, d_1, d_2, …, d_D

In Fig. 1(a), we illustrate the function $g_{LB}(n)$ for $m = 3$, $k = 10$, and $P_F = 10^{-7}$. As expected based on §IV-B, $g_{LB}(n)$ decreases with increasing n. Since $MTTF_{LB}$ depends on $g_{LB}(n)$, the key idea is to ensure that points $d_0, d_1, d_2, \ldots, d_D$ are sufficient to trace the shape of function $g_{LB}(n)$, and that the magnitude of $g_{LB}(n)$ is negligible beyond $n = d_D$.

The first point d_0 was set to $(k-m+1)$, as mentioned in §V. To compute the last point d_D, *i.e.*, the point at which $g_{LB}(n)$ becomes negligible, we observed the logarithm of function $g_{LB}(n)$ for $n \in \{1, 10^1, 10^2, 10^3, \ldots\}$. That is, we plotted the function $g_{LB}(n)$ on a logarithmic scale for both the x- and y-axes as in Fig. 1(b), and then determined the time instant at which the curve starts falling rapidly (*e.g.*, $d_D \approx 10^{55}$ in Fig. 1(b)). The intermediate points $d_1, d_2, \ldots, d_{D-1}$ were chosen such that the step size $d_{i+1} - d_i$ between any two consecutive points d_i and d_{i+1} **(i)** is small enough to closely track the function $g_{LB}(n)$, and **(ii)** yet still proportional to the order of magnitude of d_i, to avoid evaluating an exponential number of points. For example, while generating Fig. 1, the step size was 1 for $n \in (10, 100]$ and 10^{52} for $n \in (10^{53}, 10^{54}]$.

B. $MTTF_{LB}$ versus $MTTF_{sim}$

To compare $MTTF_{LB}$ and $MTTF_{sim}$, we chose specific parameters that ensure that the simulation completes within reasonable time. In particular, we avoided parameters for which $MTTF_{LB}$ was very high (typically, configurations with a very small P_F), since the number of rounds in each simulation trial for such parameters would likely be very high as well. In Fig. 2, we illustrate the results for each $P_F \in \{10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}\}$, $k \in \{5, 7, 10\}$, and m such that $k - m + 1 = 3$, *i.e.*, $m \in \{3, 5, 8\}$ (respectively).

The simulations were run on a 16-core Intel Xeon E5-2667 v2 machine. For each $P_F \in \{10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}\}$, we ran $640,000$, $64,000$, $6,400$, and 640 simulation trials, respectively. To ensure that the number of trials for each simulation was sufficient, we also computed the 99% confidence interval for each $MTTF_{sim}$ (shown as error bars in Fig. 2). In general, the smaller the P_F, the higher was the time to finish a single simulation trial. The average times required to complete a *single* simulation trial and the analytical lower bound $MTTF_{LB}$ for different values of P_F are illustrated in Fig. 3 below. While the former grows exponentially in $log\, P_F$, the latter grows linearly in $log\, P_F$.

We draw the following conclusions from the experiments. **(1)** For each configuration, $MTTF_{LB}$ and $MTTF_{sim}$ are roughly of the same order of magnitude, which indicates that the proposed method is sufficiently accurate. Note that while evaluating system reliability, the order of magnitude of the reliability metric (in this case, MTTF) is typically more important than minor differences in absolute value. **(2)** $MTTF_{LB}$ is always less than $MTTF_{sim}$. This was expected since we use a lower bound on the *p.d.f.*; $MTTF_{LB}$ is hence also a lower bound on the exact MTTF. **(3)** $MTTF_{LB}$ can be computed significantly faster than $MTTF_{sim}$ for low failure probabilities, and scales to parameters yielding very high MTTFs.

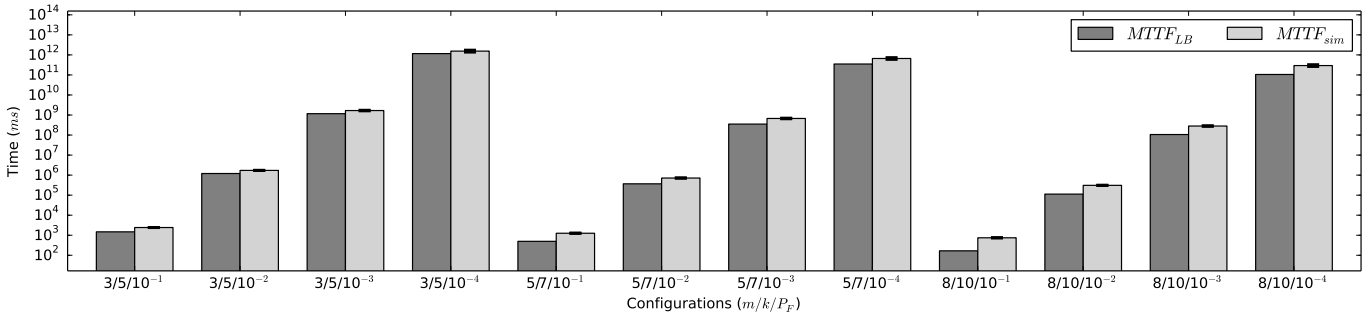


Fig. 2: The period of the system was $T = 10\,ms$. For $MTTF_{sim}$, the 99% confidence intervals are shown as error bars.

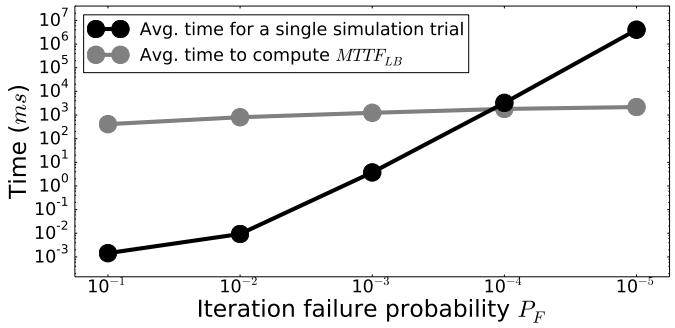


Fig. 3

Overall, the experiments show that the proposed analysis provides a fast method to compute a safe bound on the MTTF of system with (m, k) constraints. The analytical results are comparable to the simulation results, but unlike simulation, they are provably sound and scalable.

VII. Conclusion

We have proposed an analysis to derive a safe lower bound on the MTTF of a system with (m, k) constraints. MTTF is one of the standard metrics for measuring system reliability. While closed-form MTTF analyses can be derived for well-known distributions and simple system models [12, Ch. 4], the MTTF analysis for complex systems subject to different types of failures is often difficult, requiring non-trivial techniques (*e.g.*, [9, 13–15]). To the best of our knowledge, for systems with (m, k) constraints, or for the a/Con/b/c:F system model used in this paper, there exists no prior work that safely lower-bounds the system MTTF. Recent works by Eryilmaz et al. [7] and Eryilmaz and Kan [6] derive approximate MTTFs.

As mentioned before, we plan to use the presented MTTF analysis to quantify the overall reliability of a CAN-based NCS with replicated tasks that are characterized using (m, k) constraints, in the presence of environmentally-induced transient failures. We are currently developing an analysis to derive IID failure probabilities for each iteration of a control loop of the NCS. The IID property is guaranteed by the fact that we consider worst-case scenarios w.r.t. the occurrence of faults and interference, and since the iteration failure probability is obtained independently of whether earlier iterations failed, which justifies the IID assumption made in this work.

As future work, to obtain a more general analysis, we will consider systems with multiple (m, k) constraints (*e.g.*, separate constraints for delayed and incorrect messages, or for modeling short-term and long-term behavior) and systems with different flavors of (m, k) constraints (*e.g.*, out of any k *consecutive* iterations, less than m iterations may fail) [2].

References

[1] "Wolfram Mathematica: Modern Technical Computing," available at https://www.wolfram.com/mathematica/.

[2] G. Bernat, A. Burns, and A. Liamosi, "Weakly hard real-time systems," *IEEE transactions on Computers*, vol. 50, no. 4, pp. 308–321, 2001.

[3] I. Broster, A. Burns, and G. Rodriguez-Navas, "Timing analysis of real-time communication under electromagnetic interference," *Real-Time Systems*, vol. 30, no. 1-2, pp. 55–81, 2005.

[4] K.-H. Chen, B. Bönninghoff, J.-J. Chen, and P. Marwedel, "Compensate or ignore? meeting control robustness requirements through adaptive soft-error handling," in *ACM SIGPLAN Notices*, vol. 51, no. 5. ACM, 2016, pp. 82–91.

[5] J. B. Dugan and R. Van Buren, "Reliability evaluation of fly-by-wire computer systems," *Journal of Systems and software*, vol. 25, no. 1, pp. 109–120, 1994.

[6] S. Eryilmaz and C. Kan, "Dynamic reliability evaluation of consecutive-k-within-m-out-of-n:F system," *Communications in Statistics-Simulation and Computation ®*, vol. 40, no. 1, pp. 58–71, 2010.

[7] S. Eryilmaz, C. Kan, and F. Akici, "Consecutive k-within-m-out-of-n:F system with exchangeable components," *Naval Research Logistics (NRL)*, vol. 56, no. 6, pp. 503–510, 2009.

[8] A. Gujarati and B. Brandenburg, "When is CAN the weakest link? a bound on failures-in-time in CAN-based real-time systems," in *RTSS*. IEEE, 2015, pp. 249–260.

[9] P. Gupta and M. Sharma, "Reliability and MTTF evaluation of a two duplex-unit standby system with two types of repair," *Microelectronics Reliability*, vol. 33, no. 3, pp. 291–295, 1993.

[10] M. Hamdaoui and P. Ramanathan, "A dynamic priority assignment technique for streams with (m, k)-firm deadlines," *IEEE transactions on Computers*, vol. 44, no. 12, pp. 1443–1451, 1995.

[11] F. Kluge, M. Neuerburg, and T. Ungerer, "Utility-based scheduling of (m, k)-firm real-time task sets." in *ARCS*, 2015, pp. 201–211.

[12] W. Kuo and M. J. Zuo, *Optimal reliability modeling: principles and applications*. John Wiley & Sons, 2003.

[13] D. Pandey and M. Jacob, "Cost analysis, availability and MTTF of a three state standby complex system under common cause and human failures," *Microelectronics Reliability*, vol. 35, no. 1, pp. 91–95, 1995.

[14] H. Pham, A. Suprasad, and R. Misra, "Reliability and MTTF prediction of k-out-of-n complex systems with components subjected to multiple stages of degradation," *International Journal of Systems Science*, vol. 27, no. 10, pp. 995–1000, 1996.

[15] M. Ram and S. Singh, "Availability, MTTF and cost analysis of complex system under preemptive-repeat repair discipline using gumbel-hougaard family copula," *International Journal of Quality & Reliability Management*, vol. 27, no. 5, pp. 576–595, 2010.

[16] M. Sebastian and R. Ernst, "Reliability analysis of single bus communication with real-time requirements," in *PRDC*. IEEE, 2009, pp. 3–10.

[17] M. Sfakianakis, S. Kounias, and A. Hillaris, "Reliability of a consecutive k-out-of-r-from-n:F system," *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 442–447, 1992.

[18] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault tree handbook with aerospace applications," 2002.

[19] D. H. Stamatis, *Failure mode and effect analysis: FMEA from theory to execution*. ASQ Quality Press, 2003.

[20] S. Stanley, "MTBF, MTTR, MTTF & FIT explanation of terms," *IMC Networks*, 2011.