CTA: A CORRELATION-TOLERANT ANALYSIS OF THE DEADLINE-Failure PROBABILITY OF DEPENDENT TASKS

Filip Marković, Pierre Roux, Sergey Bozhko, Alessandro V. Papadopoulos, and Björn B. Brandenburg
PROBABILISTIC ANALYSIS OF REAL-TIME SYSTEMS

Why is it relevant?

Many systems have **soft** real-time guarantees rather than **hard** ones

Many systems are **not statically** analyzable but rather **statistically**

Many soft real-time systems **do not benefit** from deterministic analysis as it would **unnecessarily** over-provision system resources

Many **safety standards** are defined in terms of **failure probabilities**

---

**Question 14** For the most time-critical functions in the system, roughly how frequently can the deadline of a function be missed without causing a system failure. (n = 101)

- Not a concern: 7%
- More often than 1 in 10: 13%
- 1 in 10 to 1 in 100: 17%
- 1 in 100 to 1 in 1000: 6%
- 1 in 1000 to 1 in 1 million: 8%
- 1 in 1 million to 1 in 1 billion: 6%
- Never: 15%
- I do not know: 38%

---


OPEN PROBLEM: DEPENDENCE

Real-time systems run **intrinsically dependent** tasks, while plenty of analyses assume **independent** task execution.

“Unfortunately, the computation times of individual requests are **not statistically independent**. In the system studied here, the computation times of requests in each task are **correlated** with that of requests in many other tasks…”

“… As a consequence, the probability of meeting deadlines thus computed may be **overly optimistic**.”

“Issues of **dependence** are of **great importance** in probabilistic schedulability analysis.”

“… Analyses are needed that can address dependencies.”

We present a **Correlation-Tolerant Analysis**

DEADLINE-FAILURE PROBABILITY (DFP)

The probability that a job of a task fails to complete before its deadline.

Consider a simple system comprising two tasks

- grey task (high priority),
- blue task (low priority).

Ground-truth behavior: all possible evolutions

- Arrivals of $\tau_1$ and $\tau_2$
- Deadline of $\tau_2$
DEADLINE-FAILURE PROBABILITY (DFP)

The probability that a job of a task fails to complete before its deadline.

Consider a simple system comprising two tasks
- grey task (high priority),
- blue task (low priority).

Ground-truth behavior: all possible evolutions

\[ \begin{align*}
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{no failure} & & & & & & & & & & (\text{prob 0.96}) \\
1 & \overset{1}{\downarrow} & 2 & \overset{0}{\downarrow} & & & & & & & & \\
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{no failure} & & & & & & & & & & (\text{prob 0.005}) \\
3 & \overset{1}{\downarrow} & 2 & \overset{0}{\downarrow} & & & & & & & & \\
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{no failure} & & & & & & & & & & (\text{prob 0.005}) \\
5 & \overset{1}{\downarrow} & 2 & \overset{0}{\downarrow} & & & & & & & & \\
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{failure} & & & & & & & & & & (\text{prob 0.01}) \\
3 & \overset{1}{\downarrow} & 8 & \overset{0}{\downarrow} & & & & & & & & \\
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{failure} & & & & & & & & & & (\text{prob 0.01}) \\
5 & \overset{1}{\downarrow} & 8 & \overset{0}{\downarrow} & & & & & & & & \\
0 & \quad 1 & \quad 2 & \quad 3 & \quad 4 & \quad 5 & \quad 6 & \quad 7 & \quad 8 & \quad 9 & \quad 10 \\
\text{failure} & & & & & & & & & & (\text{prob 0.01}) \\
\end{align*} \]

\( \tau_1 \text{ executes} \quad \tau_2 \text{ executes} \quad \text{arrivals of } \tau_1 \text{ and } \tau_2 \quad \text{deadline of } \tau_2 \)
DEADLINE-FAILURE PROBABILITY (DFP)

The probability that a job of a task fails to complete before its deadline.

Consider a simple system comprising two tasks
- grey task (high priority),
- blue task (low priority).

Ground-truth behavior: all possible evolutions

- no failure (prob 0.96)
- no failure (prob 0.01)
- no failure (prob 0.005)
- failure (prob 0.01)
- failure (prob 0.01)

\( \tau_1 \) executes \( \tau_2 \) executes

\( \uparrow \) arrivals of \( \tau_1 \) and \( \tau_2 \)

\( \downarrow \) deadline of \( \tau_2 \)
DEADLINE-Failure Probability (DFP)

The probability that a job of a task fails to complete before its deadline.

Consider a simple system comprising two tasks

- grey task (high priority),
- blue task (low priority).

The ground-truth DFP of the blue task is **0.02**.

Ground-truth behavior: all possible evolutions
**DFP ANALYSIS**

Analysis that derives an upper bound on the DFP of any job of a task.

**Input:** model parameters → the easier to obtain, the better

**Output:** DFP upper bound

**Goal:** Efficient and accurate DFP

*Efficient:* minimize space and time complexity

*Accurate:* minimize over-approximation
PRIOR WORK ON DFP ANALYSIS
DFP ANALYSIS ASSUMING INDEPENDENCE

Computation of the DFP (blue task) using per-task distributions and assuming independence

Input: measured per-task execution-time distributions

Analysis: assumes independence

Output: 0.000875 < 0.02 (ground-truth DFP)

Conclusion: Ignoring task dependence (correlation) risks unsound DFP estimation.
pWCET: PESSIMISM “BAKED IN”

A distribution designed to “hide” dependence while being analytically convenient.

**Input:** Probabilistic Worst-Case Execution Time (pWCET)

Ground-truth behavior

**Analysis:** assumes independence

Output: **0.533333 > 0.02**

**Conclusion:** pWCET-based analysis can be inherently pessimistic.
SUMMARY

Ignoring correlation can be **unsound**, while pWCET-based approaches can be **overly pessimistic**.

---

**ground-truth** DFP: 0.02

**pWCET**-based DFP: 0.5333 (overly pessimistic)

**independence-assuming** DFP: 0.000875 (unsound estimate)

Also, **pWCET** derivation is not trivial

---

**per-task** ground-truth execution distributions

- 0.965
- 0.015
- 0.02

- 1
- 3
- 5

---

**pWCET** distributions

- 0.2
- 0.4
- 0.4

- 0.333
- 0.666

---

**What is enough padding?**
THIS PAPER:
A CORRELATION-TOLERANT ANALYSIS
(Not using pWCET!)
CANTELLI’S INEQUALITY

Given a random variable with a known expected value and standard deviation and some threshold $t$, it bounds the exceedance probability.

**Input:** expected value and variance of some random variable $X$.

But how does this translate to our RT problem?

$$\forall t > \mathbb{E}(X), \quad \mathbb{P}[X > t] \leq \frac{(\sigma(X))^2}{(\sigma(X))^2 + \left(t - \mathbb{E}(X)\right)^2}$$

The probability that the response-time exceeds the deadline

Response-time distribution of a task

Relative deadline

Expected value of the response-time distribution of a task

Variance of the response-time distribution of a task
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We can apply Cantelli’s Inequality to a sum of possibly correlated random variables.

\[ \Pr[X > t] \]

Response-time distribution of a task

The probability that the response-time exceeds the deadline

Relative deadline
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We can apply Cantelli’s Inequality to a sum of possibly correlated random variables.

\[ X = \sum_{j \in \text{jobs}} X_j \]

The probability that the response-time exceeds the deadline

Relative deadline

Response-time distribution of a task

The probability that the response-time exceeds the deadline
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We apply the same substitution to the rest of the inequality.

The probability that the response time exceeds the deadline

Distribution of an interfering job

Relative deadline

The probability that the response time exceeds the deadline
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We apply the same substitution to the rest of the inequality.

\[ X = \sum_{j \in \text{jobs}} X_j \]

\[ \forall t > \mathbb{E}(X), \quad P \left( \sum_{j \in \text{jobs}} X_j > t \right) \leq \frac{(\sigma[X])^2}{(\sigma[X])^2 + (t - \mathbb{E}[X])^2} \]

The probability that the response time exceeds the deadline

Distribution of an interfering job

Relative deadline

The probability that the response time exceeds the deadline
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We apply the same substitution to the rest of the inequality.

∀ \( t > \mathbb{E} \left[ \sum_{j \in \text{jobs}} X_j \right] \),

\[
\mathbb{P} \left( \sum_{j \in \text{jobs}} X_j > t \right) \leq \frac{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 + \left( t - \mathbb{E} \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}
\]
A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

We apply the same substitution to the rest of the inequality.

\[
P \left( \sum_{j \in \text{jobs}} X_j > t \right) \leq \frac{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 + \left( t - \mathbb{E} \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}
\]
What is the expected value of the sum of possibly correlated random variables?

\[ \forall t > \mathbb{E}\left[ \sum_{j \in \text{jobs}} X_j \right] \]

\[ \mathbb{P}\left[ \sum_{j \in \text{jobs}} X_j > t \right] \leq \frac{\left( \sigma\left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}{\left( \sigma\left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 + \left( t - \mathbb{E}\left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2} \]
What is the expected value of the sum of possibly correlated random variables?

\[ \forall t > \mathbb{E} \left[ \sum_{j \in \text{jobs}} X_j \right] \]

\[ \mathbb{P} \left[ \sum_{j \in \text{jobs}} X_j > t \right] \leq \frac{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2}{\left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 + \left( t - \mathbb{E} \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2} \]
EXPECTATION OF THE SUM

What is the expected value of the sum of possibly correlated random variables?

**Equal to** the sum of per-RV expected values.

\[
\forall t > \mathbb{E}\left[\sum_{j \in \text{jobs}} X_j\right],
\]

\[
\mathbb{P}\left[\sum_{j \in \text{jobs}} X_j > t\right] \leq \frac{\left(\sigma\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2}{\left(\sigma\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2 + \left(t - \mathbb{E}\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2}
\]

- The probability that the response time exceeds the deadline.
- Distribution of an interfering job.
- Relative deadline.
- Lineararity of expectation.
- Expected value of an interfering job.
- Expected value of the response time distribution.
What is the expected value of the sum of possibly correlated random variables?

**Equal to** the sum of per-RV expected values.
**EXPECTATION OF THE SUM**

What is the expected value of the sum of possibly correlated random variables?

*Equal to* the sum of per-RV expected values.

\[
\forall t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j],
\]

\[
P\left(\sum_{j \in \text{jobs}} X_j > t\right) \leq \frac{\left(\sigma\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2}{\left(\sigma\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2 + \left(t - \sum_{j \in \text{jobs}} \mathbb{E}[X_j]\right)^2}
\]

The **probability** that the response time **exceeds** the **deadline**

Distribution of an **interfering job**

Relative **deadline**

Expected value of an **interfering job**
VARIANCE OF THE SUM

What is the value of the variance of the sum of possibly correlated random variables?

∀t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j],

Variance of the response-time distribution

\leq \left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 + \left( t - \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \right)^2

Distribution of an interfering job

The probability that the response time exceeds the deadline

Relative deadline

Expected value of an interfering job
**What is the value of the variance of the sum of possibly correlated random variables?**

\[
\forall t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j], \quad \mathbb{P}\left[\sum_{j \in \text{jobs}} X_j > t\right] 
\]

**Variance of the response-time distribution**

\[
\text{Var} = \left(\sigma\left[\sum_{j \in \text{jobs}} X_j\right]\right)^2 + \left(t - \sum_{j \in \text{jobs}} \mathbb{E}[X_j]\right)^2
\]

**Standard deviation of an interfering job**

\[
\sigma\left[\sum_{j \in \text{jobs}} X_j\right]
\]

**Expected value of an interfering job**

\[
\mathbb{E}[X_j]
\]

**Distribution of an interfering job**

The probability that the response time exceeds the deadline

**Relative deadline**

\[
\leq \left(\sum_{j \in \text{jobs}} \sigma[X_j]\right)^2
\]

**Cauchy-Schwarz Inequality**
VARIANCE OF THE SUM

What is the value of the variance of the sum of possibly correlated random variables?

Less than or equal to the sum of per-RV standard deviations.

∀ \( t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \),

\[
\mathbb{P} \left( \sum_{j \in \text{jobs}} X_j > t \right) \leq \left( \sigma \left[ \sum_{j \in \text{jobs}} X_j \right] \right)^2 \leq \sum_{j \in \text{jobs}} \sigma [X_j]^2
\]

Distribution of an interfering job

The probability that the response time exceeds the deadline

Variance of the response-time distribution

Relative deadline

Cauchy-Schwarz Inequality

Expected value of an interfering job

Standard deviation of an interfering job

VARIANCE OF THE SUM

What is the value of the variance of the sum of possibly correlated random variables?

Less than or equal to the sum of per-RV standard deviations.
What is the value of the variance of the sum of possibly correlated random variables?

Less than the sum of per-RV standard deviations.

The probability that the response time exceeds the deadline

∀ \( t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \),

\[
P\left( \sum_{j \in \text{jobs}} X_j > t \right) \leq \frac{ \left( \sum_{j \in \text{jobs}} \sigma[X_j] \right)^2 + \left( t - \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \right)^2 }{2}.
\]
Now, we can use the expected values and standard deviations of the individual, possibly correlated random variables.

The probability that the response time exceeds the deadline

\[ \forall t > \sum_{j \in \text{jobs}} \mathbb{E}[X_j], \]

\[ \mathbb{P}\left[ \sum_{j \in \text{jobs}} X_j > t \right] \leq \frac{\left( \sum_{j \in \text{jobs}} \sigma[X_j] \right)^2}{\left( \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \right)^2 + \left( t - \sum_{j \in \text{jobs}} \mathbb{E}[X_j] \right)^2} \]
THERE IS MUCH MORE IN THE PAPER

Concentration Inequality
- based on Cantelli’s Ineq,
- Verified in Coq.

Ground-Truth System Model
- jobs aborted upon deadline miss
- fully-preemptive scheduling
- fixed priority, uniprocessor

Correlation-Tolerant Analysis (CTA)
- connects the other two pillars
- soundly-upper bounds DFP
- closed-form solution
LET US APPLY CTA TO THE EXAMPLE

**Input:** expected value and standard deviation upper bounds on task execution time distributions.

\[
\begin{align*}
\mathbb{E}(\begin{array}{c}
1 \\
3 \\
5
\end{array}) &= 1.11 \leq 1.12 \\
\mathbb{E}(\begin{array}{c}
2 \\
8
\end{array}) &= 2.15 \leq 2.16 \\
\sigma(\begin{array}{c}
1 \\
3 \\
5
\end{array}) &\approx 0.606 \leq 0.61 \\
\sigma(\begin{array}{c}
2 \\
8
\end{array}) &\approx 0.937 \leq 0.94
\end{align*}
\]

\[\text{deadline} = 10\]
**LET US APPLY CTA TO THE EXAMPLE**

**Input:** expected value and standard deviation upper bounds on task execution time distributions.

\[
\begin{align*}
\mathbb{E}(135) &= 1.11 \leq 1.12 & \sigma(135) &\approx 0.606 \leq 0.61 \\
\mathbb{E}(28) &= 2.15 \leq 2.16 & \sigma(28) &\approx 0.937 \leq 0.94 & \text{deadline} = 10
\end{align*}
\]

**Analysis:**

\[
P[X > t] \leq \frac{(\sigma(X))^2}{(\sigma(X))^2 + (t - \mathbb{E}(X))^2}
\]
CTA: A Correlation-Tolerant Analysis of the Deadline-Failure Probability of Dependent Tasks

**LET US APPLY CTA TO THE EXAMPLE**

**Input:** expected value and standard deviation upper bounds on task execution time distributions.

\[
\begin{align*}
\mathbb{E}(\text{1 3 5}) &= 1.11 \leq 1.12 \\
\mathbb{E}(\text{2 8}) &= 2.15 \leq 2.16 \\
\sigma(\text{1 3 5}) &\approx 0.606 \leq 0.61 \\
\sigma(\text{2 8}) &\approx 0.937 \leq 0.94 \\
\text{deadline} &= 10
\end{align*}
\]

**CTA:**

\[
\mathbb{P}[\text{1 3 5} + \text{2 8} > 10] \leq \frac{(0.61 + 0.94)^2}{(0.61 + 0.94)^2 + (10 - (1.12 + 2.16))^2} \approx 0.05
\]
LET US APPLY CTA TO THE EXAMPLE

The CTA-derived DFP over-approximates the ground-truth DFP, being more accurate than pWCET-DFP.

**Input:** expected value and standard deviation upper bounds on task execution time distributions.

\[
\mathbb{E}(\begin{bmatrix} 1 & 3 & 5 \end{bmatrix}) = 1.11 \leq 1.12 \quad \sigma(\begin{bmatrix} 1 & 3 & 5 \end{bmatrix}) \approx 0.606 \leq 0.61 \\
\mathbb{E}(\begin{bmatrix} 2 & 8 \end{bmatrix}) = 2.15 \leq 2.16 \quad \sigma(\begin{bmatrix} 2 & 8 \end{bmatrix}) \approx 0.937 \leq 0.94 \quad \text{deadline} = 10
\]

**CTA:**

\[
\mathbb{P}[\begin{bmatrix} 1 & 3 & 5 \end{bmatrix} + \begin{bmatrix} 2 & 8 \end{bmatrix} > 10] \leq \frac{(0.61 + 0.94)^2}{(0.61 + 0.94)^2 + (10 - (1.12 + 2.16))^2} \approx 0.05
\]

**Output:**

- **ground-truth** DFP: 0.02
- **pWCET-based** DFP: 0.5333 (overly-pessimistic)
- independence-assuming DFP: 0.000875 (unsound estimate)
EVALUATION
EVALUATION

How does CTA compare to the pWCET-based analyses in general?

We compared CTA to the following baselines:

- **Berry–Esseen**: DFP lower bound computed with the Berry-Esseen theorem.
- **Chernoff**: DFP upper bound computed with Chernoff bound

---


EVALUATION SETUP

Synthetic task sets were randomly generated to highlight differences between pWCET and CTA analysis.

Four experiments were conducted to investigate:

1. Influence of the task set size on DFP,
2. The influence of the expected utilization according to pWCET distributions,
3. The influence of the expected utilization according to CTA inputs,
4. The influence of the maximum standard deviation on CTA.

In this talk, we focus on (1)
EVALUATION, EXPERIMENT 1

*Investigating the influence of the task-set size*

As the number of tasks in a set **increases**, the CTA method's **advantage** over pWCET-based baselines **grows**.

This is because pWCET can be overly pessimistic in the presence of correlations.

The level of pessimism increases at a faster rate than the expectation used by CTA with new interfering tasks.
EVALUATION, EXPERIMENT 1

*Investigating the influence of the task-set size*

CTA derives better bounds than Chernoff

\[ \approx 88\% \]

Range of DFP solutions for Chernoff

CTA derives worse bounds than Chernoff

\[ \approx 12\% \]

Range of DFP solutions for CTA

CTA typically offers lower bounds, but its reliance on simple summary statistics can limit the range of obtainable DFP bounds.
SUMMARY
SUMMARY

Efficient: minimize space and time complexity

- CTA relies on a closed-form expression; its run-time and space complexity are negligible
- CTA tolerates dependence by construction
- CTA does not require pWCET nor any similar independence-implying construct

Accurate: minimize over-approximation

- The results are promising, but pWCET can still be useful under certain conditions.

A novel analysis with a lot of potential.