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



RTSS 2023 December 8, 2022

Filip Marković, Pierre Roux, Sergey Bozhko, Alessandro V. Papadopoulos, and Björn B. Brandenburg



MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS



 \mathbf{N}



European Research Counci Established by the European Commission

Vetenskapsrådet





PROBABILISTIC ANALYSIS OF REAL-TIME SYSTEMS

Why is it relevant?



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

[1] Akesson et al. *RTSJ* (2022)

MPI-SWS, ONERA, MDU

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

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

The total utilization of that system goes above 100%. Using response time analysis in such situation automatically yields unbounded (infinite) worst-case response times.

[2]

SIL	Low demand mode	Continuous/High demand mode		
	prob. failure on demand	prob. failure per hour		
1	$\geq 10^{-2}$ to < 10^{-1}	$\geq 10^{-6}$ to < 10^{-5}		
2	$\geq 10^{-3}$ to < 10^{-2}	$\geq 10^{-7}$ to < 10^{-6}		
3	$\geq 10^{-4}$ to < 10^{-3}	$\geq 10^{-8}$ to < 10^{-7}		
4	$\geq 10^{-5}$ to < 10^{-4}	$\geq 10^{-9}$ to < 10^{-8}		

Table 1: IEC 61508: Permitted Failure Probabilities

[3]

[2] Rivas et al. *WATERS* (2016) [3] Agrawal et al. *ICCAD* (2020)

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* "... As a consequence, the probability of *independent*. In the system studied here, meeting deadlines thus computed may be the computation times of requests in each overly optimistic." task *are correlated* with that of requests in many other tasks..." [1] [1] *"Issues of <u>dependence</u> are of* "... Analyses *are needed* that <u>great importance</u> can address <u>dependencies</u>." in probabilistic schedulability analysis." CTA: A Correlation-Tolerant Analysis of the [2] [2] Deadline-Failure Probability of Dependent Tasks re Roux² Sergey Bozhko^{1,3} Alessandro V. Papadopoulos Planck Institute for Software Systems (MPI-SWS), German ²ONERA/DTIS, Université de Toulouse, France fälardalen University (MDU), Sweder alysis (CTA). pendent. The primary mechanism for realizing such an analysi ics of each task's grou per bounds on the mean and CIA does not use pWCET, nor does it require the full execution-time distribution to be known. Core parts of the analysis have been verified with the Coq proof assistant. Empirical comparison with state-of-the-art WCDFP analyses reveals that CTA can yield significantly improved bounds (e.g., a lower WCDFP than any pWCET-based method for $\approx 70\%$ of the workloads tested at 90% pWCET utilization and 60% average utilization). Beyond accuracy gains, the favorable results highlight the potential of the previously unexplored analytical direction underlying CTA. We present a **Correlation-Tolerant Analysis** lead to considerable pessimism compared to actual behavior I. INTRODUCTION Probabilistic analysis of real-time systems holds the promise This paper. Exploring a fundamentally different direction, w of addressing the central challenge of modern hardware and propose a novel correlation-tolerant analysis (CTA) of WCDF under fixed-priority scheduling. CTA is based on Cantelli's behavior of real-time tasks. Such uncertainty in the execution in the fabric of modern computing systems, more often than not procludes not use pWCET, nor does it otherwise in the faoric of modern computing systems, more orten than hot precludes meaningful (classical) worst-case analysis, leaving a stochastic perspective as the only viable option. stochastic perspective as the only viable option. One of the most pressing open problems in this space is the issue of *dependent* execution times (also referred to as the issue of *dependent* execution times (also referred to as the issue of *dependent* execution times (also referred to as execution-time *correlation*). Specifically, when bounding a task's *worst-case deadline-failure probability* (WCDFP), it is not account for possible dependencies on both previous Notably, CTA also does not require the degree of inter- or intracrucial to account for possible dependencies on both previous activations (*inter-task dependence*) and other tasks in the system (*intra-task dependence*). If such dependencies are ignored, the WCDFP may be severely under-approximated. We convey the core idea with a simple example (Sec. II These observations are not new: the lack of independence From Cantelli's inequality [9], we derive, and verify with Coq [13, 41], an upper bound on the sum of random in practice was recognized as a safety problem already more than 25 years ago by Tia et al. [49] in one of the first works variables with unknown degrees of correlation (Sec. IV). on probabilistic schedulability analysis. Unfortunately, only little progress has been made on this issue since Tia et al.'s · We formally model the execution of a stochastic sporad real-time workload under preemptive uniprocessor fixed



[1] Tia et al. *RTAS* (1995) [2] Davis and Cucu-Grosjean *LITES* (2019)

MPI-SWS, ONERA, MDU

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

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



F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

MPI-SWS, ONERA, MDU

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

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 **4**-<u>the easier to obtain, the better</u> **Output**: DFP upper bound **Goal**: Efficient and accurate DFP

minimize Efficient:



space and **time** complexity

minimize over-approximation Accurate:



MPI-SWS, ONERA, MDU



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



Ground-truth behavior

per-task ground-truth execution-time distributions

Analysis: assumes independence

0.965	0.015	0.02		0.975	0.025	
1	3	5	+	2	8	=

Output: 0.000875 < **0.02** (ground-truth DFP)

Conclusion: Ignoring task dependence (correlation) risks unsound DFP estimation.

MPI-SWS, ONERA, MDU



PWCET: PESSIMISM "BAKED IN"

A distribution designed to "hide" dependence while being analytically convenient.

Input: Probabilistic Worst-Case Execution Time (pWCET)



Analysis: assumes independence



Output: 0.533333 > 0.02

Conclusion: pWCET-based analysis can be inherently pessimistic.

MPI-SWS, ONERA, MDU

SUMMARY

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







MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

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



Sergey Bozhko^{1,2} Filip Marković¹ Georg von der Brüggen³ Björn B. Brandenburg ¹Max Planck Institute for Software Systems, Germany ²Saarbrücken Graduate School of Computer Science, Saarland University, Germany ³Department of Computer Science, TU Dortmund University, Germany

Abstract—The concept of a probabilistic worst-case execution time (pWCET) has gradually emerged from the work of many authors over the course of 2-3 decades. Intuitively, pWCET is a simplifying model abstraction that safely over-approximates the pround-truth probabilistic execution time (pET) of a real-time task, in particular, when analyzing the cumulative processor demand of multiple jobs, the pWCET abstraction is intended to allow for the use of techniques from probability theory that require from the use of techniques from probability theory that require time independent and identically distributed (IID), even though the underlying ground-truth pET random variables are usually not independent. Howver, while powerful the pWCET concept is subtle and difficult to define precisely, and easily misinterpreted. To place the pWCET motes to suitable for formal proof. In addition, an adequacy property is stated that performally copating three states in the probability theory that performand proof. In addition, an adequacy property is stated that performal proof. In addition, an adequacy property is on an "IID upper bound pET." The proposed pWCET definition of pMCET for the part is the tother by the first approvale probability theory performant performant considering multiple jobs executing in temporal proximity, their pETs are decidedly nor independent random variables. pET?" The proposed pWCET definition is shown to satisfy this their pETs are decidedly not independent random variables the IID guarantee is form and proofs have been verified with the Coq proof assistant.

I. INTRODUCTION

Whether by choice or necessity, interest in probabilistic real-time systems is on the rise. By choice, because there are good reasons to prefer a stochastic perspective (e.g., cost become a dominant method in the probabilistic toolbox. Upon are good reasons to prefer a stochastic perspective (e.g., cost considerations when dealing with soft or "firm" workloads that can tolerate the occasional deadline violation). Or by necessity because the complexities of today's commodify hardware because the transition of today's commodify hardware because the complexities of today's commodity hardware platforms (such as multi-level caches, speculative execution or undisclosed component specifications) quite often prevent a meaningful *worst-case execution time* (WCET) analysis, leaving measurement-based approaches as the only available option. Either way, real-world systems—subject to market its met the prerequisites for traditional worst-case guarantees. Now, if absolute certainty is unatainable given the circum-stances, then the next best guarantee is bounds on the proba-bility of undesirable events (*e.g.*, missed deadlines). Howver, while the motivation and benefits are clear, the problem of actually obtaining such bounds is far from trivial and, as we

actually obtaining such bounds is far from trivial and, as we in validating its adequacy as a "safe upper bound." review in Sec. II, has been the subject of intense study [18, 19]. In response to this challenge, the notion of *probabilistic* **Contributions.** In this paper, we:

worst-case execution time (pWCET) has emerged over the past
• observe that the currently accepted pWCET definition has in new work in this area. Intuitively, pWCET is a simplifying

offician, and thereby is the first notion of pWCKT for guarantee is formally established. All definitions guarantee is formally established. All definitions guarantee is formally established. All definitions guarantee is formally established and provide the pWCET abstraction promises a convenient way out [16]: by substituting all pET random variables with random variables following suitably chosen pWCET distributions, one obtains a problem composed only of independent and iden distributed (IID) random variables, which opens the door to a wealth of classic techniques from probability theory.

Given these advantages, it is no wonder that pWCET has



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: <u>expected value</u> and <u>variance</u> of some random variable X.

But how does this translate to our **RT problem**?



MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

Variance of the response-time distribution of a task

Expected value 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.



MPI-SWS, ONERA, MDU

A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

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



MPI-SWS, ONERA, MDU

A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

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



MPI-SWS, ONERA, MDU

A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

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



MPI-SWS, ONERA, MDU

A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

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



$$\frac{\left(\sigma\left[\sum_{j\in jobs} X_{j}\right]\right)^{2}}{\left[\left[jobs X_{j}\right]\right]^{2} + \left(t - \mathbb{E}\left[\sum_{j\in jobs} X_{j}\right]\right)^{2}}$$

A SUM OF POSSIBLY CORRELATED RANDOM VARIABLES

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



MPI-SWS, ONERA, MDU

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

$$= jobs X_j \left[\begin{array}{c} & \\ & \\ \\ & \\ \end{array} \right]^2 + \left(t - \mathbb{E}\left[\sum_{j\in jobs} X_j\right]\right)^2$$

EXPECTATION OF THE SUM

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



MPI-SWS, ONERA, MDU

EXPECTATION OF THE SUM

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



MPI-SWS, ONERA, MDU

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.



F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

Expected value of the response time

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.



MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

Expected value of the response time

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.



MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

$$\frac{\left(\sigma\left[\sum_{j\in jobs} X_{j}\right]\right)^{2}}{\left[=jobs X_{j}\right]^{2} + \left(t - \sum_{j\in jobs} \mathbb{E}\left[X_{j}\right]\right)^{2}}$$

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?



MPI-SWS, ONERA, MDU

VARIANCE OF THE SUM

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



MPI-SWS, ONERA, MDU

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.



MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

Standard deviation of an interfering job

Cauchy-Schwarz Inequality

 $\sigma \left[\sum_{j \in jobs} \right]$ X_j j∈jobs $\sum_{j \in jobs}$ E

VARIANCE OF THE SUM

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

Less than the sum of per-RV standard deviations.



F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

Standard deviation of an interfering job

 $\sum_{j\in jobs} \sigma$ + $\left(t-\sum_{j\in jobs}\mathbb{E}\left[X_{j}\right]\right)$ σX_j

CORRELATION-TOLERANT INEQUALITY

Now, we can use the expected values and standard deviations of the individual, possibly correlated random variables.



MPI-SWS, ONERA, MDU



THERE IS MUCH MORE IN THE PAPER



MPI-SWS, ONERA, MDU

LET US APPLY CTA TO THE EXAMPLE

Input: <u>expected value</u> and <u>standard deviation</u> upper bounds on task execution time distributions.



F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

8) $\approx 0.937 \le 0.94$ deadline = 10

LET US APPLY CTA TO THE EXAMPLE

Input: <u>expected value</u> and <u>standard deviation</u> upper bounds on task execution time distributions.



Analysis:

 $\mathbb{P}[X > t] \le \frac{(\sigma(X))}{(\sigma(X))^2 + (t)^2}$

$$\frac{(X)^2}{t - \mathbb{E}(X)^2}$$

LET US APPLY CTA TO THE EXAMPLE



MPI-SWS, ONERA, MDU

LET US APPLY CTA TO THE EXAMPLE

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



MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg

pWCET-based DFP: 0.5333 (overly-pessimistic)

EVALUATION

EVALUATION

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

We compared **CTA** to the following baselines: **Berry–Essen**: DFP lower bound computed with the Berry-Esseen theorem. **Chernoff**: DFP upper bound computed with Chernoff bound

Analytical Approximations in Probabilistic Analysis of Real-Time Systems

Filip Marković^{1,2}, Thomas Nolte¹, and Alessandro Vittorio Papadopoulos¹ Mälardalen University (MDU), Sweden ²Max Planck Institute for Software Systems (MPI-SWS), German

Abstract—Probabilistic timing and schedulability analysis of real-time systems is constrained by the problem of often in-tractable exact computations. The intractability problem is present whenever there is a large number of entities to be enabled and accurately derive an enabled and accurately derive an enabled of the large free mathematical derives and the larg

analysed, e.g., jobs, tasks, etc. In the last few years, the analytical upper bound on the probability that a distribution (e.g., of an

proximations for deadline-miss probability emerged as an aportant solution in the above problem domain. In this paper, we explore analytical solutions for two major roblems that are present in the probabilisty is of real-time stems. First, for a safe approximation of the entire probability istributions (e.g., of the accumulated execution workloads) we how how the Berry-Fissen theorem can be used. Second we hoeffding [26] and Bernstein bound [3], as shown by von der Hoeffding [26] and Bernstein bound [3], as shown by von der

tasks increases. The methods are compared with the circular convolution approach. We also investigate the memory footprint comparison between the proposed Berry-Esseen-based solutions and the circular convolution. The contributions and results pre-sented in this paper complement the starter the starter starter between the probabilistic response time analysis are the tractability of the analysis ind the circular convolution. The contributions and results pre-sented in this paper complement the state-of-the-art in accurate and efficient probabilistic analysis of real-time systems. *Index Terms*—probabilistic timing analysis, probabilistic schedulability analysis, analytical bounds, Berry-Esseen theorem (Section 3.2, p.18): "In contrast to classical task models, task sets containing a number of tasks with execution times described by random variables can usefully have a total worst The analysis of hard real-time systems has been built on case processor utilisation that exceeds 1. This means that there the foundations of various mathematical concepts such as an- is a backlog, meaning outstanding task execution with a finite alytical bounds, fixed-point recursions, Linear Programming, probability of occurrence, at the end of each hyperperiod. This etc. Among the most important concepts being used, there are backlog makes the analysis of probabilistic response times for the linear and non-linear bounds which allow for efficient and each job in the hyperperiod much more complex". Therefore, accurate analysis of different aspects of real-time systems, e.g., we formulate Problem 2, the first problem addressed in this paper.

This problem is also relevant in areas such as probabilistic However, the majority of real-time systems exhibit an cache and WCET analysis [17], [36] (see [19] for a more execution time that is typically lower than the estimated comprehensive list), and for this reason, we stated the problem worst-case, which often leads to the corresponding resource in a more general form. In Problem 2, the term intractability provisioning being pessimistic. Diverse research efforts have considers the computation demands in terms of space (membeen devoted to overcoming such pessimism while provid- ory) and time, which cannot be met by computing the exact specifically, in recent years, analytical bounds on deadline based approaches). This is a common problem, as identified

anstributions (e.g., of the accumulated execution workloads) we show how the Berry-Esseen theorem can be used. Second, we propose an approximation built on the Berry-Esseen theorem for efficient computation of the quantile functions of probability execution distributions. We also show the asymptotic bounds the execution distribution of the fixed-priority preemptive tasks. In the evaluation, we investigate the complexity and accuracy of the proposed methods as the number of analysed jobs and there are also problems that directly benefit from the computa-tion of the entire probabilistic response time distributions, task workloads and their cumulative distribution functions (CDES)

I. INTRODUCTION

feasibility, schedulability, resource bandwidth, etc.

When hard real-time systems are considered, the bounds must be deterministic. The evolution of bound-based analysis started from the seminal paper by Liu and Layland [28], result. ing in many analytical bounds for various model assumptions, or a response-time) whose exact computation is intractable? e.g. [2], [7], [9], [25].

ing tools for analysing relevant real-time properties. More distributions (e.g., using the linear or circular convolution-

[1] Marković et al. *RTSS* (2022)

MPI-SWS, ONERA, MDU

F. Marković., P. Roux., S. Bozhko., A. V. Papadopoulos and B. B. Brandenburg



Efficient Computation of Deadline-Miss Probability and Potential Pitfalls

Kuan-Hsun Chen, Niklas Ueter, Georg von der Brüggen, and Jian-Jia Chen Department of Informatics, TU Dortmund University, Germany E-mail: {kuan-hsun.chen, niklas.ueter, georg.von-der-brueggen, jian-jia.chen} @tu-dortmund.de

Abstract—In soft real-time systems, applications can tolerate algorithm on a uniprocessor system. Suppose that S_t is the rare deadline misses. Therefore, probabilistic arguments and analyses are applicable in the timing analyses for this class of systems, as demonstrated in many existing researches. Convolutionems, as demonstrated in many existing researches. Convolution-based analyses allow to derive tight deadline-miss probabilities, Chernoff bounds while, on the other hand, ensure a tighter approximation since a larger variable space can be searched more efficiently, i.e., by using binary search techniques over a larger area instead of a sequential search over a smaller

I. INTRODUCTION

the respective outputs within given timing constraints. Hard runtime efficiency as reported in [18]. ime constraints are necessary if any deadline miss may soft-error recovering systems, where soft errors that occur the performance of the aforementioned approaches. during a task's execution trigger error-recovery routines. Based Motivational Example: Consider a real-time embedded sysmiss metric.

Now, the probability that a task τ_i is not finished at time i but suffer from a high time complexity. Among the analytical approaches, which result in a significantly faster runtime than the topological transfer and transfer and the topological transfer and transfe he tightest results. In this paper, we show that calculating the leadline-miss probability using Chernoff bounds can be solved by considering an equivalent convex optimization problem. This allows us to, on the one hand, decrease the runtime of the probability consult of S_t . Previous job-level convolution-based approaches [1], [9], [14], [16] in probabilistic response-time analyses suffered from their high time complexity, i.e., only a small number of tasks could be considered. Recently, von der Brüggen et al. [18] proposed a ranger area instead of a sequential search over a smaller area. We evaluate this approach considering synthesized task-sets. Our approach is shown to be computationally efficient for large task systems, whilst experimentally suggesting reasonable approximation quality compared to an exact analysis. *Index Terms*—Deadline miss probability, Soft real-time systems approaches, the time complexity remains exponential with respect to the number of tasks. Furthermore, the experimental results presented by von der Brüggen et al. [18] show that In embedded and cyber-physical systems, timeliness is an analyzing a task system with 100 tasks can take several essential feature. The strongest timeliness requirement is to hours. Chen and Chen in [7] proposed to use Chernoff bounds provide hard real-time guarantees. That is, all computing entities must not only be correct functionally, but also compute

The Chernoff b lead to catastrophic consequences. However, many embedded for any real number s > 0. While the Chernoff bound is an systems can still be functionally correct for occasional, i.e., over-approximation with no non-trivial analytical guarantees quantified and bounded, deadline misses. The relevance of for the approximation quality, the quality varies with the these classes of systems to industry is evident from safety choice of s. Hence, in order to optimize the approximation standards such as IEC-61508 [11] and ISO-26262 [12] that quality, it is beneficial to find the smallest Chernoff bound ef require (very) low failure probability but not necessarily a ficiently, based on all possible s values. The following example failure probability of zero. Further examples of relevance are motivates the studied problem in this paper, and demonstrates

on the probabilistic characteristic of the soft error occurrences, tem with a set of sporadic tasks, i.e., $\Gamma = \{\tau_1, \tau_2, \cdots, \tau_{25}\}$, on the task system exhibits probabilistic behavior. In these cases, a uniprocessor. We follow a similar setup as described in [7], probabilistic task models and analyses can help the system [17], [18]. That is, a task has two modes with associated designer to achieve expectedly high system utilization, whilst probabilities, where a mode is characterized by its worstquantifying the probabilistic system behavior using a deadline- case execution time (WCET). Such a setting is common when software based fault-tolerance techniques are considered, i.e. We consider sporadic real-time task systems, in which a α a task au_i has a normal execution mode with a related WCET sporadic task τ_i releases an infinite number of task instances, C_i^N and probability \mathbb{P}_i^N as well as an abnormal execution called jobs, that are separated by a minimum inter-arrival time mode with WCET C^A and associated probability \mathbb{P}^A . Further, T_i . All tasks are scheduled under a preemptive fixed-priority $C_i^N \leq C_i^A$, $\mathbb{P}_i^A < \mathbb{P}_i^N$, and $\mathbb{P}_i^N = 1 - \mathbb{P}_i^A$. We use the

[2] Chen et al. *DATE* (2019)

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.

MPI-SWS, ONERA, MDU

EVALUATION, EXPERIMENT 1

Investigating the influence of the task-set size



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

MPI-SWS, ONERA, MDU

- solutions for CTA

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.

MPI-SWS, ONERA, MDU