Trace-Based Statistical Timing Analysis of Complex Industrial Real-Time Embedded Systems

Yue Lu
Mälardalen Real-Time Research Centre (MRTC), Västerås, Sweden
yue.lu@mdh.se

***Abstract*—Real-time embedded systems are becoming ever more complex, and we are reaching the stage where even if static Response-Time Analysis (RTA) was feasible from a cost and technical perspective, the results are overly pessimistic making them less useful to the practitioner. When combined with the fact that most timing analysis tends to be statistical in nature, this suggests there should be a move toward statistical RTA, which gives a task's worst-case response time estimate under a predictable probability of being exceeded. However, to make such analysis useful, it is imperative that we have evidence that the statistical RTA and the information analyzed is sufficiently accurate. In this project, we will address the above issue by presenting and validating a statistical RTA technique based around analyzing timing traces taken from real systems, which can cope with systems that are complex from both a size and tasks' dependencies perspective, as well as some typical case when the source code and/or object code of systems is/are withheld due to the protection of intellectual property.**

***Keywords*-complex industrial real-time embedded systems; task execution and temporal dependencies; statistical response-time analysis; timing traces; single processor;**

I. Motive for the Research

Many industrial embedded systems are very complex, large, flexible, and highly configurable software systems. Such systems often consist of millions of lines of code, and contain hundreds of tasks, many are with real-time constraints and being triggered by other tasks in a complex and nested pattern. More importantly, in such systems, tasks may have intricate dependencies in their temporal behavior, such as 1) asynchronous message-passing and globally shared state variables, which may decide important control-flow conditions with major impact on task execution time as well as task response time, 2) task offsets, and 3) runtime changeability of priorities and periods of tasks. Consequently, the systems have a very complicated runtime behavior. We refer to systems with such characteristics as *Complex Industrial Real-Time Embedded Systems* (CIRTES). Examples of such systems include the robotic control system IRC 5, developed by ABB [1], as well as several telecom systems.

To maintain, analyze and reuse CIRTES is very important, difficult and expensive, which, nonetheless, offers high business value responding to great concern in industry. For instance, one specific problem in maintenance, i.e., modifying the system after delivery to correct faults, improve performance or other attributes, or to adapt the product to a changed environment, is the risk for introducing timing-related errors. In particular, for the CIRTES in safety-critical applications, both functional and non-functional correctness are often equally important. Thus, temporal behavior, e.g., Worst-Case Response Time (WCRT) of the adhering tasks in systems has to be known. For instance, a failing industrial robot could halt an entire production line in a factory for hours, causing a huge financial loss. Software bugs that lead to slow response time in Anti-lock Brake System (ABS) in cars could cause loss of human lives, and recall of several hundreds of thousands of vehicles. In this project, we focus on Response-Time Analysis (RTA) of CIRTES in safety-critical applications.

In order to determine that all timing constraints (deadlines) are met in all circumstances, RTA is often used in the context. Traditional RTA methods [2] are under the assumption that tasks are independent with each other, and the longest computation time of adhering tasks in a system can be bounded and known. Such bounds on the task Worst-Case Execution Time (WCET) are given by WCET analysis [3] which is fundamental to RTA methods in terms of providing the inputs to RTA. In order to perform safe analysis covering system worst-case scenarios, static WCET analysis is adopted, which increases the degree of pessimism in the RTA results, i.e., absolute guarantees in terms of single numerical values of tasks' WCRT. Typically, such RTA results are too pessimistic to be practically applied. We refer such RTA methods which return an absolute WCRT guarantee as *deterministic* RTA.

Probabilistic approaches [4], [5], [6] can reduce the pessimism, in which tasks' execution times are modeled by *independent and identically distributed (i.i.d)* discrete random variables. Such probabilistic guarantees offer significant advantages over deterministic approaches which attempt to make absolute guarantees, thereby severely limiting the opportunity of use of advanced hardware features and inevitably attaining lesser performance. However, none of them can model and analyze CIRTES, due to the existence of adhering intricate task execution dependencies that we mentioned previously.

Other methods which adopt resource reservations algorithms such as the CBS [7] usually requires the exact

knowledge of the entire distributions of the computation times and the inter-arrival times of the tasks, which are in generally impossible to obtain. Real-Time Queueing Theory (RTQT) [8] also provides a way to compute tasks' response time distributions using various real-time scheduling algorithms, under the *heavy traffic assumption* which significantly restricts its application in practice. Moreover, preemption between customers is not permitted in RTQT.

Our previous work has used simulation-optimization based methods [9], [10] and model checking-based approaches [11]. However, each of these is limited by the validity of the models [12], [13] that they heavily depend on. Typically, when the source code and/or object code are/is not available to access due to the protection of intellectual property in CIRTES, the application of such analysis methods is devastated totally.

The state of practice in industry is that many companies developing CIRTES have no means for timing analysis, and are forced to rely on testing to find timing-related problems. Nonetheless, all timing errors can in most cases not be detected in *unit testing* as they only occur in the integrated system, when concurrent activities are interacting or interfering, under a very specific condition. Moreover, if errors related to timing and concurrency effects are discovered in testing of the entire system, they are typically hard to reproduce. Worse yet, it is not only extremely difficult and expensive to test all scenarios in the system, but also hard to predict how a product will be used. Enabling RTA of CIRTES is a problem of high industrial relevance thereof.

II. Problem Setting

Based around our study of the state-of-the-art RTA, the main focus of this project is to investigate to use statistical methods in RTA of CIRTES which are large systems with millions of lines of code and hundreds of adhering tasks, and contain intricate task execution and temporal dependencies. Moreover, such methods should not rely on the access to the source code and/or object code of systems, as pertaining intellectual property issue may be the typical case when the construction of CIRTES is done by using different prefabricated software (known as *components*) from different vendors, which is a continuously increasing trend. As a result, it is our intention to timing traces taken from real systems and then process them with more powerful statistical techniques, in terms of not only giving accurate estimates of worst-case behaviors, but also allowing the validity of the results to be considered. From the perspective of research questions, there are five problems identified in this project and introduced as follows.

Problem P1*: How to collect qualified analysis samples in order to make satisfied, the most important assumption required by statistics and probability theory, i.e., all the observations in statistical inference have to be independent and identically distributed?*

Motivation for P1: Due to the existence of intricate task execution and temporal dependencies in CIRTES, an upcoming Response Time (RT) data may not be independent with the RT data previously measured during the real execution of the system, for the same task. Further, the pertaining timing behavior of the adhering tasks is also quite complicated. As shown in [12], [13], given a large number at sampling data, the *Probability Density Function* (PDF) histogram of the RT sampling distribution of the CTRL task (i.e., the most important task under analysis) in one example of CIRTES (i.e., a robotic control system developed by one of our industrial partners), is clearly conforming to a multi-modal distribution having several peaks. Specifically, because of such distinctive feature of our target CIRTES, it is difficult to bring conventional statistical methods [14] (e.g., t-test, z-test and analysis of variance (ANOVA)) into the context of predicting the worst-case timing behavior of the CTRL task in CIRTES. Since one basic assumption, i.e., the underline population is assumed to follow a normal distribution cannot be satisfied. More importantly, a new way of constructing tasks' RT sampling distributions has to be introduced, in order to collect samples as qualified observations which fulfill the basic assumption *Independent and Identically Distributed* (i.i.d.) required by any statistical inference in probability theory and statistics.

Problem P2*: Based around the qualified analysis samples, what kind of statistical methods can be used in RTA of Complex Industrial Real-Time Embedded Systems, which are large systems with millions of lines of code and hundreds of adhering tasks, and contain intricate task execution and temporal dependencies, such as asynchronous message-passing, globally shared state variables, tasks with offset and changeability of tasks' period and priority at runtime?*

Motivation for P2: After obtaining qualified observations in tasks RT sampling distributions under analysis (which conform to the i.i.d. assumption required by statistics and probability), the proposed statistical method should be able to predict the system worst-case behavior from the perspective of task response time. In other words, the proposed method based around the statistical inference should be able to give accurate estimates of the *tail behavior* of the underlying populations which are represented by the sampling distributions used in the statistical inference.

Problem P3*: How confidence in the results given by the proposed statistical method can be obtained and understood?*

Motivation for P3: Statistics use samples to draw inferences about the estimate of certain parameters of the population represented [15]. Such inferences are conducted by using the hypothesis test which is at the certain level of significance. In other words, there might be some *type-I* or *type-II*

error [16][1] appearing in the statistical inference used by our proposed method, which diminishes the confidence in the corresponding results. In this project, we also address this issue by first presenting a mathematical way of obtaining such confidence in results given by the proposed analysis method, in terms of probabilities. Next, we validate the method by using extensive validation using information from real industrial control systems.

Problem P4*: What kind of the evaluation models should be used in the method validation?*

Motivation for P4: As our target systems are CIRTES, the evaluation models should not be so simple, e.g., the system model containing independent tasks. Further, with the purpose of method validation, the exact value of WCRT of tasks under analysis has to be known through some other analysis methods, other than traditional RTA. Consequently, such evaluation models should contain subset of intricate task execution and temporal dependencies that we previously mentioned, which results in lower complexity when compared to CIRTES and the derivation of the known actual WCRT of tasks under analysis. The referenced methods which are used to obtain such exact WCRT of tasks under analysis in the evaluation models can be simulation-optimization based methods proposed in our prior work [9], [10]. In addition, some case studies based around testing the real CIRTES which are available on side of our industrial partners will be also considered.

III. Overview of Our Solutions and the Current Results

The specific in-depth technical contribution of the project is the framework for trace-based statistical timing analysis of CIRTES, i.e., *RapidRT*. The analysis framework ideally should provide an accurate WCRT estimate of tasks on focus pertaining to a statistical constrain, i.e., a certain predictable probability. Further, such WCRT estimate could bound the actual WCRT of tasks when it is known. Based around the outcomes of our research at current stage, the overview of our research and pertaining research results in the project are summarized as follows:

- **C1** *A New Sampling Mechanism for Collecting Timing Traces Taken from Real Systems* is proposed and presented in [17], [13], which tackles the issue about the i.i.d. assumption required by statistics and probability theory. **C1 gives the answer to the research question P1**.
- **C2** *A Statistical RTA of CIRTES* that could be considered as a pragmatic approach in the context. In particular, the proposed method based around Extreme Value Theory (EVT) [18] and other statistical techniques, produces a WCRT estimate using response time data samples from measurements of the real system, under a statistical constraint, i.e., a certain probability of being exceeded. The obtained estimate has potential of being considered as an accurate upper bound on WCRT estimates of tasks in CIRTES. The proposed method is evaluated by using simulation models inspired by two real industrial control applications as shown in [19]. **C2 gives the answer to the research question P2**. At our latest research stage, we present the mathematical way of calculating the confidence in the analysis results given by our method, which **gives the answer to the research question P3**.
- **C3** *Validation of Our Proposed Method by using Information from Real Industrial Control Systems* that is done by using a set of evaluation models inspired by a robotic control application developed by one of our industrial partners. In addition, the actual WCRT of tasks in such evaluation models can be obtained through our simulation-based analysis methods presented in our prior work [9], [10]. **C3 provides the answer to the research question P4**.
- **C4** *Optimization Process about Obtaining More Accurate Analysis Results* that is in development at our current research stage. This will improve our proposed analysis method from the perspective of accuracy of analysis results, as well as computation time consumed by the method.
- **C5**[2] *A Set of Prototyping Tools* implementing the ideas from C1-C4.
  At our current research stage, we developed a prototype of RapidRT as an executable program with a simple Graphical User Interface (GUI) by using Microsoft's C# programming language and .NET framework 2.0. The GUI for the tool is shown by Figure 1.

IV. Summary

In this paper, we have presented our project which is about trace-based timing analysis of Complex Industrial Real-Time Embedded Systems (CIRTES). To be specific, we have described a project overview, formulated research questions and pertaining motivations, as well as introduced research results at current stage. Our future work will mainly focus on the method validation, improvements and case studies by using real systems available on side of our industrial partners.

Acknowledgment

This work was partially supported by the Swedish Foundation for Strategic Research (SSF) and the Swedish Research Council (VR).

[1] A Type I error is often referred to as a *false positive*, and is the process of incorrectly rejecting the null hypothesis in favor of the alternative; A Type II error is the opposite of a Type I error and is the false acceptance of the null hypothesis.

[2] C5 is not a scientific contribution.

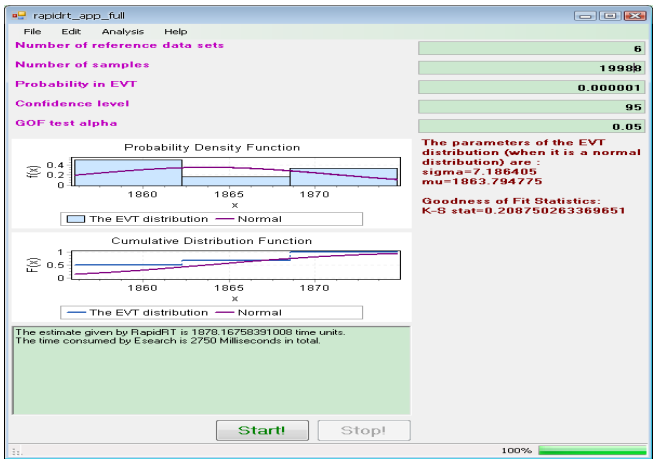

Figure 1. The Graphical User Interface (GUI) for RapidRT.

REFERENCES

[1] "www.abb.com, 2011."

[2] *Handbook of Real-Time and Embedded Systems*. Chapman and Hall/CRC (July 23, 2007), 2007.

[3] R. Wilhelm, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, and P. Stenström, "The worst-case execution-time problem—overview of methods and survey of tools," *Trans. on Embedded Computing Sys.*, vol. 7, no. 3, pp. 1–53, 2008.

[4] A. Burns, G. Bernat, and I. Broster, "A Probabilistic Framework for Schedulability Analysis," in *Proceedings of the 3rd International Conference on Embedded Software (EMSOFT' 03*, 2003, pp. 1–15.

[5] L. Cucu-Grosjean, "Probabilistic real-time schedulability analysis: from uniprocessor to multiprocessor when the execution times are uncertain," RR-INRIA, Tech. Rep., May 2009.

[6] J. M. López, J. L. Díaz, J. Entrialgo, and D. García, "Stochastic analysis of real-time systems under preemptive priority-driven scheduling," *Real-Time Syst.*, pp. 180–207, November 2008.

[7] L. Abeni, G. Buttazzo, S. Superiore, and S. Anna, "Integrating Multimedia Applications in Hard Real-Time Systems," in *Proceedings of the 19th IEEE Real-time Systems Symposium*, 1998, pp. 4–13.

[8] J. E. K. Rusty O. Baldwin, Nathaniel J. Davis IV and S. F. Midkiff, "Real-time queueing theory: A tutorial presentation with an admission control application," *Queueing Systems*, vol. 35, no. 1-4, pp. 1–21, 2000.

[9] M. Bohlin, Y. Lu, J. Kraft, P. Kreuger, and T. Nolte, "Simulation-Based Timing Analysis of Complex Real-Time Systems," in *Proceedings of the 15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA' 09)*, August 2009, pp. 321–328.

[10] J. Kraft, Y. Lu, C. Norström, and A. Wall, "A Metaheuristic Approach for Best Effort Timing Analysis targeting Complex Legacy Real-Time Systems," in *Proceedings of the 14th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS' 08)*, Apr. 2008.

[11] Y. Lu, T. Nolte, I. Bate, and C. Norström, "Timing Analyzing for Systems with Task Execution Dependencies," in *Proceedings of the 34th Annual IEEE Computer Software and Applications Conference (COMPSAC' 10)*. IEEE, July 2010.

[12] Y. Lu, J. Kraft, T. Nolte, and I. Bate, "A statistical approach to simulation model validation in response-time analysis of complex real-time embedded systems," in *The 26th ACM Symposium on Applied Computing (SAC'11)*. ACM, March 2011.

[13] Y. Lu, T. Nolte, I. Bate, J. Kraft, and C. Norström, "Assessment of trace-differences in timing analysis for complex real-time embedded systems," in *The 6th IEEE International Symposium on Industrial Embedded Systems (SIES' 11)*, IEEE, Ed. IEEE, June 2011.

[14] "t-test and ANOVA, http://mathworld.wolfram.com, 2010."

[15] D. S. Moore, G. P. Mccabe, and B. A. Craig, *Introduction to the practice of statistics*, 6th ed. New York, NY 10010: W. H. Freeman and Company, 2009.

[16] "Website of EXPERIMENTAL ERRORS: TYPE I ERROR - TYPE II ERROR," www.experiment-resources.com/type-I-error.html.

[17] Y. Lu, J. Kraft, I. Bate, and T. Nolte, "A Statistical Approach to Simulation Model Validation in Response-Time Analysis of Complex Real-Time Embedded Systems," in *Proceedings of The 26th ACM Symposium on Applied Computing (SAC' 11)*. ACM, March 2011.

[18] E. Gumbel, *Statistics of Extremes*. Columbia University Press, 1958.

[19] Y. Lu, T. Nolte, J. Kraft, and C. Norström, "A Statistical Approach to Response-Time Analysis of Complex Embedded Real-Time Systems," in *Proceedings of the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA' 10)*, August 2010.