

# Chapter 12

## A Model–Driven Engineering Method for DRE Defense Systems Performance Analysis and Prediction

**Katrina Falkner**

*The University of Adelaide, Australia*

**Nickolas Falkner**

*The University of Adelaide, Australia*

**Vanea Chiprianov**

*The University of Adelaide, Australia*

**Claudia Szabo**

*The University of Adelaide, Australia*

**Gavin Puddy**

*The University of Adelaide, Australia*

### ABSTRACT

*Autonomous, Distributed Real-Time Embedded (DRE) defence systems are typically characterized by hard constraints on space, weight, and power. These constraints have a strong impact on the non-functional properties of the final system, especially its performance. System execution modeling tools permit early prediction of the performance of model-driven systems; however, the focus to date has been on the practical aspects and creating tools that work in specific cases, rather than on the process and methodology applied. In this chapter, the authors present an integrated method to performance analysis and prediction of model-driven DRE defense systems. They present both the tools to support the process and a method to define these tools. The authors explore these tools and processes within an industry case study from a defense context.*

### BACKGROUND

Mission-critical Distributed Real-time and Embedded (DRE) systems, such as naval combat systems or mission-systems, can have life-cycles that can be counted in the decades (Falkner, 2013). The design complexity and cost of such long-lived large systems continue to grow while

business owners continue to seek improvements in the return on investments for such projects. While an understanding of both functional and non-functional aspects of the system design is important, issues associated with the non-functional aspect of the design are of greater concern for resource-constrained platforms, such as submarines or autonomous vehicles. With strict budget

DOI: 10.4018/978-1-4666-6194-3.ch012

allocations for space, weight and power for various systems installed in such platforms, any early insight into the performance of these systems, and their corresponding deployment and budget considerations, becomes crucial.

Prediction of software performance has developed from early approaches based on abstract models to *Model-Driven Engineering* (MDE) based approaches (Woodside, 2007a). MDE operates through the definition of *Domain Specific Modeling Languages* (DSMLs), which are used to develop *models* that encapsulate the essential requirements of the problem space at a high level of abstraction, using abstractions that fit the domain of the problem space, and are hence more understandable to domain experts. MDE follows a process by which these models are transformed, either manually or automatically, through stages of increased specificity and detail, eventually resulting in the provision of an executable software system.

MDE techniques are typically applied to the development of application software components, but may also be used to model and solve the configuration and deployment phases, as well as system execution emulation, testing and analysis. *System Execution Modeling* (SEM) (Hill, 2010), a recent development from research into measurement-based performance prediction, provides detailed early insight into the non-functional characteristics of a DRE system design. A SEM-based approach supports the evaluation of overall (software) system performance, incorporating component interactions and the performance impact of 3rd party software such as middleware. These approaches are based upon simple models of resource consumption from the component's "business logic" (Hill, 2010; Paunov, 2006) and support detailed performance modeling of software systems, enabling predictions of performance through execution of representative source code of behavior and workload models deployed on realistic hardware test-beds.

SEM and MDE may be used in combination to support the emulation of system components and performance models, enabling performance data to be used to redesign and reconfigure the system, prior to any construction of the corresponding real system (Falkner, 2013). This is becoming increasingly important with the trend towards the development of *open* DRE systems, which must support frequent and rapid evolution, changes in component integration, communication partners and respond to run-time changes (Trombetti, 2005). The use of MDE, DSMLs, automatic code generation and utilisation of off-the-shelf technologies has enabled the SEM approach to abstract the development complexities of DRE systems, while still ensuring detailed performance insight to the level required to provide performance evaluation of mission-critical systems.

## RELATED WORK

There are numerous works on model-based performance engineering, including comprehensive surveys (Balsamo, 2004; Smith, 2007; Koziolok, 2010; Isa, 2011) that explore the many individual systems, approaches and methodologies and case studies. (Koziolok, 2010) presents a survey of both model- and measurement-based approaches performance prediction and evaluation for component-based systems, classifying the main prediction approaches in five categories: based on UML (among which those based on the UML profiles SPT and MARTE (Espinoza, 2006)), based on proprietary meta-models, focused on middleware, formal approaches, and measurement approaches. In this categorisation, our method would most likely be part of the category of approaches based on proprietary meta-models. (Balsamo, 2004) presents a survey of model-based performance prediction approaches, while (Becker, 2006) provides an overview of performance modeling and measurement methods for component-based systems

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/a-model-driven-engineering-method-for-defense-systems-performance-analysis-and-prediction/116114](http://www.igi-global.com/chapter/a-model-driven-engineering-method-for-defense-systems-performance-analysis-and-prediction/116114)

## Related Content

---

### A Voice-Enabled Framework for Recommender and Adaptation Systems in E-Learning

A. A. Azeta, C. K. Ayoand N. A. Ikhu-Omoregbe (2013). *Integrated Models for Information Communication Systems and Networks: Design and Development* (pp. 71-96).

[www.irma-international.org/chapter/a-voice-enabled-framework-for-recommender-and-adaptation-systems-in-e-learning/79659](http://www.irma-international.org/chapter/a-voice-enabled-framework-for-recommender-and-adaptation-systems-in-e-learning/79659)

### Service-Oriented Design Process Using UML

Steve Latchemand David Piper (2005). *Service-Oriented Software System Engineering: Challenges and Practices* (pp. 88-108).

[www.irma-international.org/chapter/service-oriented-design-process-using/28951](http://www.irma-international.org/chapter/service-oriented-design-process-using/28951)

### Analysis of Existing Software Cognitive Complexity Measures

Sanjay Misra, Adewole Adewumi, Robertas Damaseviciusand Rytis Maskeliunas (2017). *International Journal of Secure Software Engineering* (pp. 51-71).

[www.irma-international.org/article/analysis-of-existing-software-cognitive-complexity-measures/204524](http://www.irma-international.org/article/analysis-of-existing-software-cognitive-complexity-measures/204524)

### CSPM: Metamodel for Handling Security and Privacy Knowledge in Cloud Service Development

Tian Xia, Hironori Washizaki, Yoshiaki Fukazawa, Haruhiko Kaiya, Shinpei Ogata, Eduardo B. Fernandez, Takehisa Kato, Hideyuki Kanuka, Takao Okubo, Nobukazu Yoshiokaand Atsuo Hazeyama (2021). *International Journal of Systems and Software Security and Protection* (pp. 68-85).

[www.irma-international.org/article/cspm/269522](http://www.irma-international.org/article/cspm/269522)

### Cyber Security in Drone Technology

T. Kumaran, R. Jaganraj, K. Arunkumar, B. Kirubaduraiand A. Backiyaraj (2023). *Cyber-Physical Systems and Supporting Technologies for Industrial Automation* (pp. 152-163).

[www.irma-international.org/chapter/cyber-security-in-drone-technology/328497](http://www.irma-international.org/chapter/cyber-security-in-drone-technology/328497)