Law-based Verification for Complex Swarm Systems

Rolf Drechsler[1,2] Hoang M. Le[1] Mathias Soeken[1,2] Robert Wille[1,2]

[1]Institute for Computer Science, University of Bremen, 28359 Bremen, Germany
[2]Cyber-Physical Systems, DFKI GmbH, 28359 Bremen, Germany
{drechsle,hle,msoeken,rwille}@informatik.uni-bremen.de

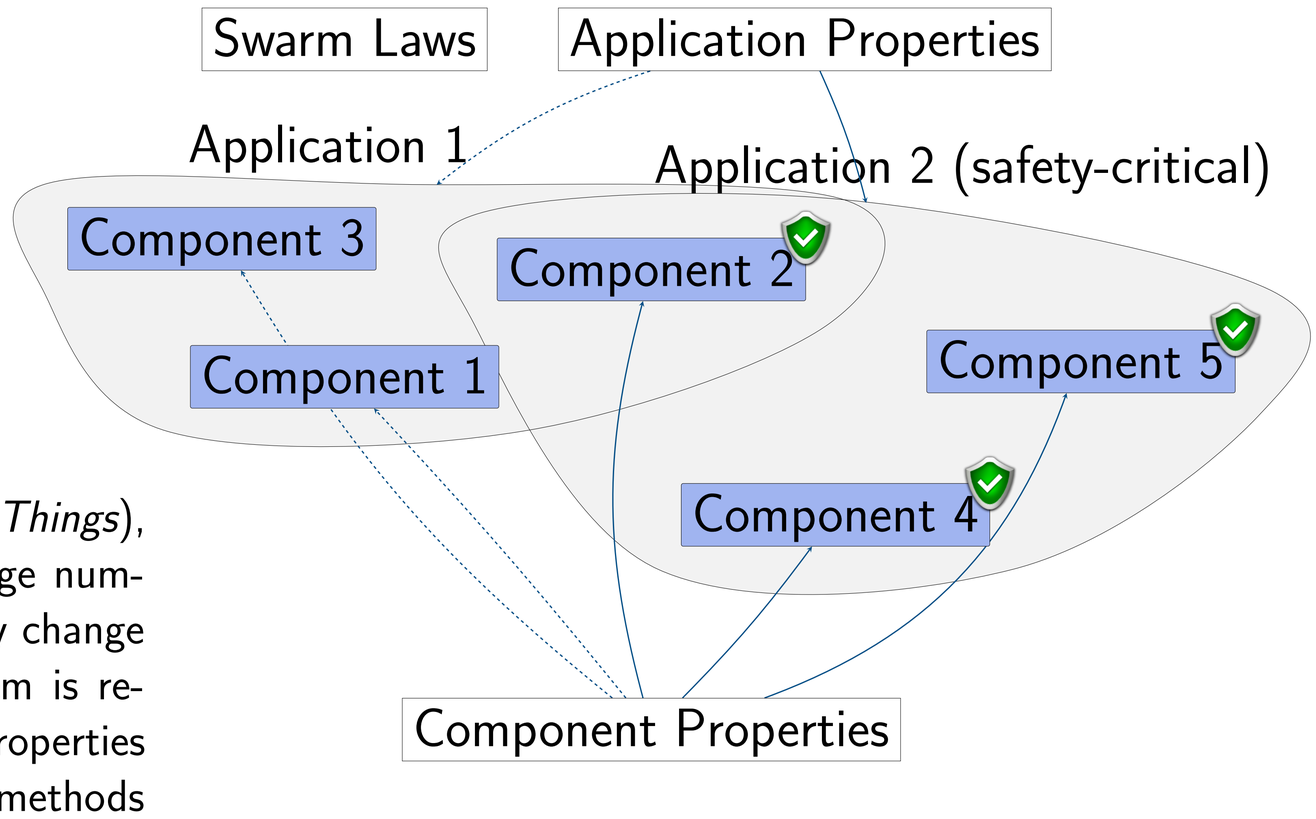
Abstract

Motivated by the recent advances with respect to the costs, size, and power consumption of electrical and sensor systems, the design of swarm systems received significant attention in the past decade. While several manifestations are investigated (including the "classical" *System of Systems* (SoS), their recent extensions to *Cyber-Physical Systems* (CPS), as well as networks such as proposed in TerraSwarm [1] and the *Internet of Things*), swarm system are commonly characterized by a large number of heterogeneous components which dynamically change their structure [1] — in the following such a system is referred to as *Complex Swarm System* (CSS). These properties pose a daunting challenge to the development of methods and solutions ensuring the correctness of these systems, i.e. to methods that check whether a given CSS indeed behaves as intended [1].

In this work, we discuss the corresponding verification challenges of these systems. In fact, checking the correctness of the components and applications of a CSS is usually not sufficient to imply the correctness of the CSS itself. Furthermore, since the functionality of a CSS is not specifically predetermined, a precise model is usually not available for verification. In order to address these issues, we propose a verification scheme that does not rely on a complete formal representation of the structure and the functionality of a CSS, but rather focuses on the verification of a set of *laws* prohibiting the components in the CSS from performing illegal actions. Based on these laws, a verification methodology is envisioned that does not require a precisely specified model anymore. The key issues of this methodology as well as resulting open research questions are discussed in this work.

Open Research Questions

- How to describe laws for incompletely specified environments?
- How to make verification feasible?
- How to trust an adaptive system?



Levels of Verification

This implicit hierarchy leads to three levels of verification:

1. *Each component* has to be verified on its own which ensures that a component functions according to its specification. This can be performed by established methods for (formal) verification such as assume-guarantee reasoning [2] or property checking [3].
2. *A CSS application* has to be verified in order to ensure that it follows a well-defined specific functionality. Since an application can just be considered as a conventional system of systems with respective subsystems and subcomponents, established compositional verification techniques can be applied for this purpose.
3. Finally, *the CSS* itself needs to be verified as the correctness of its components and its applications does not necessarily imply the correctness of the CSS. To the best of our knowledge, no verification technique exists for this purpose thus far.

References

[1] E. A. Lee *et al.*, "The TerraSwarm research center (TSRC) (A white paper)," University of California at Berkeley, Tech. Rep. UCB/EECS-2012-207, 2012.

[2] C. B. Jones, "Specification and design of (parallel) programs," in *IFIP Congress*, 1983, pp. 321–332.

[3] A. Pnueli, "The temporal logic of programs," in *Foundations of Computer Science*, 1977, pp. 46–57.