# Verifying Systems-of-Systems with Statistical Model Checking

Axel Legay, Jean Quilbeuf, Flavio Oquendo

# Verifying Systems-of-Systems with Statistical Model Checking

Axel Legay, Jean Quilbeuf and Flavio Oquendo

October 2015

Verifying the correctness of systems-of-systems (SoS) is a key challenge, largely because SoSs are evolutionarily developed by combining autonomous systems to fulfill a mission that could not be performed by one of the constituent systems alone. In the trade-off of correctness vs. scalability, model checking does not scale up to address the trustworthiness of SoSs, owing to the state explosion problem. A recent technique, however, has overcome this shortcoming: Statistical Model Checking is based on sampling traces of the system-of-interest until adequate statistical evidence has been established.

DANSE, one of the first European projects dedicated to SoS engineering, has defined a new methodology for the rigorous design of SoSs (Figure 1).

The behaviour of an SoS emerges from the interaction among its constituent systems. The DANSE methodology (co-designed by world-leaders in the SoS industry, such as THALES, EADS, and IBM) recommends that an SoSs behaviour (in terms of trustworthiness) be verified whenever a new SoS is being designed or when an existing SoS is undergoing a new evolution.

Clearly, DANSE advocates verification procedures to guarantee that an SoS accomplishes its missions in a trustworthy manner. These missions include performing a given service, which is the main reason for the SoS to exist, but also guaranteeing the quality of service, in particular in terms of safety, security and other extra-functional properties, e.g. ensuring the privacy of consumers connected to a smart grid.

Desired SoS behaviours and quality are often abstract and not verifiable, which further accentuates the difference in the DANSE methodology from systems engineering: requirements are difficult to verify and evolve with the SoS. The DANSE methodology primarily describes SoS requirements in the form of goals and contracts. Goals are quantifiable characteristics to be optimized toward an objective value. Contracts are statements that must be true for the SoS to have acceptable behaviour. Goals and contracts can be identified at both SoS and constituent system levels.

Testing will often not work in this context. Indeed, the interaction between the constituent systems is highly unpredictable, which makes it difficult to derive test cases with high coverage. Moreover, testing makes it hard to cast complex quantitative properties.

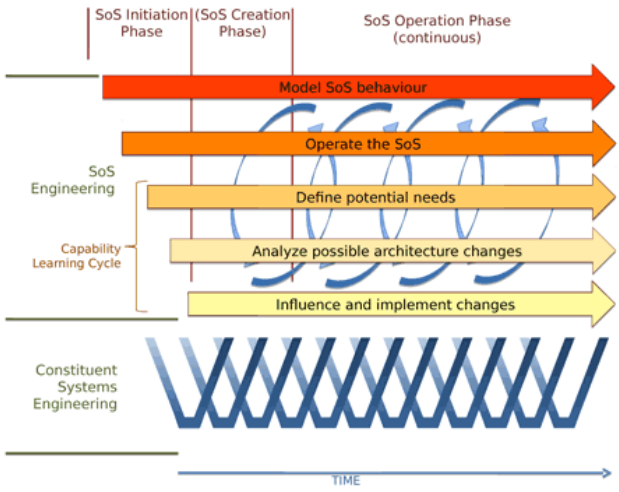


Figure 1: DANSE SoS Lifecycle.

Model checking is a widely recognized verification technique to guarantee the correctness of a system-of-interest, relying on algorithms that check whether all executions of the modeled system satisfy properties stated in a specification logic. Its use to support formal verification of SoS models is impractical, however, for several reasons. First, as an SoS is obtained by the combination of several systems, the combinatorial blow up of the state-space, commonly known as the state explosion problem, prohibits this technique from being applied to most real-world applications of SoS. Second, model checking tools typically require models to be specified in a particular language. Unfortunately, in an SoS each constituent system is usually designed using a specific modelling language (e.g. Modelica, Simulink), relying on a specific computational model. Therefore, it would be necessary to translate all constituent system models into a common formal language understandable by a model checker. But overcoming this technological issue is unlikely to solve the problem, because the state space of an SoS is too large to be handled by a model checker. Moreover, the semantics of all the constituent systems and their interactions may not be known.

To solve those issues, DANSE proposes a novel approach based on Statistical Model Checking (SMC). SMC consists of observing several executions of the system-of-interest, monitoring them with respect to a given property, and then using an algorithm from the statistics (e.g. Monte Carlo, hypothesis testing, etc.) to derive the overall probability to satisfy the property.

SMC is a compromise between testing and classical model checking techniques. Simulation-based methods are known to be far less memory- and time-intensive than exhaustive ones, and are often the only feasible possibility in the case of SoS. This method does not require extra modelling or specification effort, but simply an operational model of the SoS that can be simulated and checked

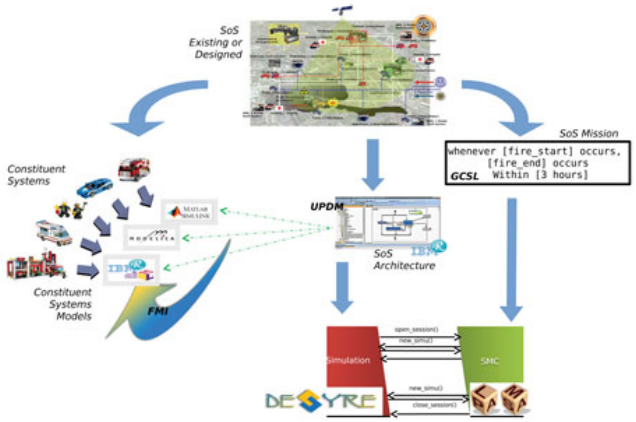


Figure 2: DANSE SoS Tools.

against state-based properties.

Within this framework, it is assumed that the next state of the SoS depends on some probability distribution. This is not a major restriction since probabilities are naturally used to model user requests and environmental states (e.g. weather conditions, traffic, human knowledge). Results from statistics provide bounds on the approximation error depending on the number of simulations, which allows fine tuning of the analysis depending on the requested precision.

SMC algorithms are implemented in the Plasma-Lab tool. This tool has been used to enable verification of SoSs in the DANSE project as depicted in Figure 2. In DANSE, the co-simulation of heterogeneous constituent systems in an SoS is obtained by relying on the FMI/FMU standard. Each constituent system model is compiled to a Functional Mockup Unit (FMU) that complies with the Functional Mockup Interface (FMI). The simulation is handled by the DESYRE simulator which orchestrates the execution of the FMUs according to the defined SoS architecture. The missions are specified as GCSL patterns that are then translated to BLTL, one of the property languages understood by Plasma-Lab. During the analysis, Plasma-Lab interacts with DESYRE to launch new simulations and control execution of the current one.

In the DANSE project, SMC has been applied to verify several complex industrial case studies. In particular, it was used to verify a water treatment and distribution system on a national scale. The mission verified that the system trustworthily provides enough water for the customer. The DANSE approach was also used to assess the reliability of an air traffic management system. In this case, SMC was used to check that the system remain operational more than 99% of the time, on a scale of 25 years.

Future work on the verification of SoSs is mainly focused on the specification and verification of emergent behaviour by tightly integrating a formal ADL for describing SoS architectures, i.e. SosADL and an enhanced Plasma-Lab.

*Links:*
`http://danse-ip.eu/`
`http://project.inria.fr/plasma-lab/`
`https://team.inria.fr/estasys/`
`http://www-archware.irisa.fr/`

# References


[1] Alexandre Arnold, Benoît Boyer, and Axel Legay. Contracts and behavioral patterns for sos: The EU IP DANSE approach. In *Proceedings 1st Workshop on Advances in Systems of Systems, AiSoS 2013, Rome, Italy, 16th March 2013.*, pages 47–66, 2013.

[2] Benoît Boyer, Kevin Corre, Axel Legay, and Sean Sedwards. Plasma-lab: A flexible, distributable statistical model checking library. In *Quantitative Evaluation of Systems - 10th International Conference, QEST 2013, Buenos Aires, Argentina, August 27-30, 2013. Proceedings*, pages 160–164, 2013.

[3] Håkan L. S. Younes and Reid G. Simmons. Statistical probabilistic model checking with a focus on time-bounded properties. *Inf. Comput.*, 204(9):1368–1409, 2006.