Compositional Systems Theory

Georgios Bakirtzis (University of Virginia)

$$\begin{tikzcd}
B(\boxed{Z}) \arrow[r, "B\phi"] \arrow[d, "\alpha_Z"'] & B(\boxed{UAV}) \arrow[d, "\alpha_{UAV}"] \\
R(\boxed{Z}) \arrow[r, "R\phi"'] & R(\boxed{UAV})
\end{tikzcd}$$

Safety & security are intertwined

I have long been fascinated by relationships between seemingly separate concepts, such as safety and security, and the emergent effects that arise from their coupling. An interesting example of such emergence is the Triton malware. Triton is the first identified attack – a violation of security – with the sole intention of disabling safety systems to instigate accidents – a violation of safety [5]. This malware makes it apparent that, unlike the security of a bank or other kinds of private information, the security of cyber-physical systems is also a safety problem. However, safety and security are often addressed individually, with little recognition of their inextricable relationship. This illustrates the need to study safety and security in unison, such that we can design resilient systems that are able to operate, even in a degraded state, without causing accidents.

Compositionality

To achieve safety and security coengineering we need high-fidelity models earlier, during the design phase of the lifecycle. This leads to one of the crucial research questions in this domain: "How might we formally model a system to address such complex metrics, like safety and security, which require a number of model views to assure their correct behavior in their eventual deployment?". Through my multidisciplinary experience I have come to the conclusion that part of the answer lies in *compositionality* – the concept of formally coupling components to model systems of increasing complexity.

This led me to take interest in the areas of *formal methods*, *systems theory*, and *diagrammatic reasoning*, with a particular focus on how they intersect in cyber-physical systems. Unification of these areas can give rise to modeling languages that better assure the safe and secure behavior of cyber-physical systems, where undesirable behaviors can lead to accidents. Towards this goal, I envision a research program that features the following thrusts.

Research goals

- Manage complexity and unify diverse system views by leveraging compositionality.
- Develop analytical tools to address the intersection of safety and security early.
- Implement prototype modeling tools employing the above theories.

Fostering collaboration is key

To reach these goals we need a merger between visualization techniques – a matter of practice – and mathematical rigour – a matter of theory. I believe this can result only by fostering a collaborative environment. To this end, I have forged long-term collaborative partnerships within a number of overlapping fields including mathematics, control, visualization, safety, and security, to name a few. This has allowed me to achieve a level of expertise in all the above fields, which would be impossible if I worked in isolation. The multidisciplinary nature of the challenges faced by cyber-physical systems makes this necessary.

For example, I brought that same multidisciplinary sensibility to my application of systems theory to cybersecurity. Specifically, I augmented well-proven hazards techniques to account for security violations [4]. While systems theory has been largely successful in finding safety violations, my work has investigated the hypothesis that systems theory is extendable to account for attacker behavior, ultimately positioning my research at the forefront of systems-theoretic security analysis. This approach originated precisely from the recognition that security violations can lead to accidents.

To be useful any unified theory of safety, security, and resilience needs to be empirically validated. To achieve such a validation we need tools that cater to both security analysts and system designers, such that there is a common modeling language between the two. This is where I am advancing diagrammatic reasoning and its associated visual interpretation. I have envisioned and implemented such tools [3], by myself and by mentoring master's students, and I have generally published and formally presented results in two disparate types of venue – security and systems engineering conferences and journals. This required me to venture into applied fields, including natural language processing, visualization, and software engineering.

Compositional systems theory

Currently, I am exploring notions of compositionality in system design for safety and security. Compositional methods explicitly consider interactions between components in order to characterize the system's behaviors. My research seeks to generalize a number of methods and relate modeling tools such that the composite assures precisely the safe and secure behavior of cyber-physical systems (often through category theory or graph transformations [2, 1]).

As Kurt Lewin said, "there is nothing as practical as a good theory". In hindsight it seems clear that compositional methods *are* the intersection of my research interests. However, because I didn't begin my journey in composionality I am equipped with a number of experiences that better position me to make advances both internally and externally to the field. Applications of this foundational work will be used to create new modeling tools that can relate the different model views necessary in cyber-physical system design.

In the future I plan on extending my current research to develop high-fidelity compositional models of cyber-physical systems. *Future research trajectory*

1. *Incorporating dynamics and control.* Different fields often decide on a diagrammatic language, for example, in control there are the so-called box diagrams. However, the diagrammatic language itself is not considered part of mathematical modeling. Compositional methods instead view the diagrammatic language as mathematical relationships. To be useful, the compositional formalism must decompose to concrete semantics. As autonomy and coordination become commonplace in cyber-physical systems, it will be increasingly important to be able to simulate a number of performance metrics but also be able to relate them with each other.
2. *Producing provable guarantees.* At the moment modeling languages are on a spectrum with respect to simulation capability and the ability to handle multiple levels of abstraction. On the one side of the spectrum, there are modeling languages that manage abstraction well but have a scarcity of simulation capabilities. On the other side there are modeling languages that work in one level of abstraction but can mathematically guarantee the behavior associated with that abstraction. Compositionality promises to bridge this gap but there is a lot of work needed to build this bridge in practice.
3. *Addressing security early in the lifecycle.* For years the security community has collected information on attack vectors, which have historically been recorded in natural language. To apply this information at the early lifecycle it is important to transform the natural language definitions into a model-based representation. Additionally, this information is often associated only with the computational units of a cyber-physical system because we mainly record attacks on information systems. An open research problem I am particularly interested in is what other information must we record to model cyber-physical attacks and in what form such that it can be used in a model-based setting.
4. *Building software for compositional modeling.* Currently, compositional methods are applied through "pen and paper". There have been some improvements in this area, particularly for software engineering, but there is still a lack of tools for modeling cyber-physical systems compositionally. I am interested in developing these tools, and more importantly, evaluating them with real engineers for their efficacy in practice.

Beyond my theoretical contributions to cyber-physical system modeling, my research is congruent with several governmental initiatives in the realm of deploying safe and secure systems [7] and industry, particularly the modeling tool sector [6]. *Impact*

References

[1] G. Bakirtzis et al. "A model-based approach to security analysis for cyber-physical systems". In: *Proceedings of the 2018 Annual IEEE International Systems Conference (SysCon 2018)*. 2018.

[2] G. Bakirtzis et al. "Data-Driven Vulnerability Exploration for Design Phase System Analysis". In: *IEEE Systems Journal* (2019).

[3] G. Bakirtzis et al. "Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis". In: *Proceedings of 15th IEEE Symposium on Visualization for Cyber Security (VizSec 2018)*. 2018.

[4] B. T. Carter et al. "A systems approach for eliciting mission-centric security requirements". In: *Proceedings of the 2018 Annual IEEE International Systems Conference (SysCon 2018)*. 2018.

[5] M. Giles. *Triton is the world's most murderous malware, and it's spreading*. `https://perma.cc/5QS8-U37C`. MIT Technology Review, 2019.

[6] Z. Scott and D. Long. *One model, many interests, many views*. Tech. rep. Vitech, 2018. URL: `http://www.vitechcorp.com/resources/white_papers/onemodel.pdf`.

[7] United States Department of Defense. *Digital engineering strategy*. Tech. rep. 2018.