Continuous-Time Computational Aspects of Cyber-Physical Security

Sam Green, İhsan Çiçek, and Çetin Kaya Koç
Department of Computer Science
University of California, Santa Barbara
{*sam.green,koc*}*@cs.ucsb.edu*
ihsancicek@engineering.ucsb.edu

***Abstract*—A wide variety of mixed digital-physical systems with complex and often loosely defined components are now deployed, whose behavior affect our daily lives in significant and sometimes critical ways. Consider that: in 2015, Ukraine experienced the first known (or publicized) hacker-caused power outage; the U.S. FDA issued a warning in regard to vulnerabilities in a medical infusion pump system; and Southern California firefighting aircraft were repeatedly grounded by interference from hobby drones. The mixed digital-physical aspect of such systems opens new and, as-of-yet, lightly explored opportunities for hybrid design, modeling, and analysis. Robust and safe systems must be designed and deployed to meet operational and security challenges. Additionally, the continuous-time nature of the physical components of these systems implies a fit for certain high-performance, low-power analog computing solutions.**

This talk attempts to survey existing efforts related to such risks and opportunities. It also ties the topics together and provides guidance to other researchers interested in exploring the hybrid aspects of mixed digital-physical systems.

***Keywords*-cyber physical systems; safety and security; analog computing**

I. Introduction to Cyber-Physical Security

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. They provide critical functionality in transportation, health care, manufacturing, and utilities. Most CPS components—particularly those of critical nature—are networked using wireless and wired communication networks, embedded processors, sensors, and actuators. They interact with humans and the rest of the physical world, deliver critical real-time data, and often must support guaranteed performance. Cyber-physical systems can provide much richer functionality, efficiency, autonomy, and reliability than manually controlled and loosely coupled systems. However, they also create inherent vulnerability related to privacy, security, robustness, and reliability of the underlying components and as a whole system. Because CPS can be significantly faster than humans or they can control and coordinate large-scale systems (such as the electrical grid), security and reliability issues are critically important.

However, as an engineering community, we have yet to mature the design, development, and analysis of cyber-physical systems. Each year, there are numerous incidents related to this fact—and we can expect to see the number of incidents increasing yearly until the international academic and industrial CPS communities mature.

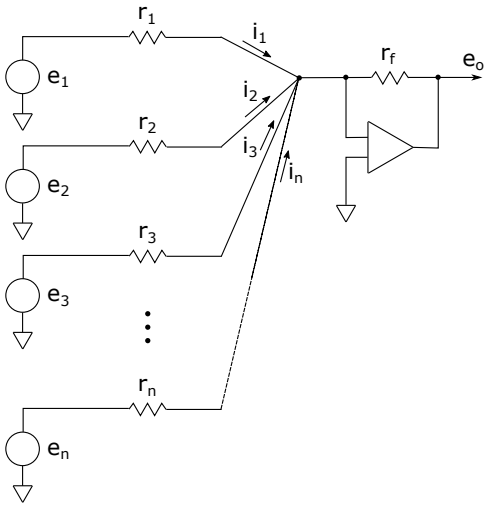

Figure 1. A dot product calculation can be accomplished with an operational amplifier-based circuit, pictured above; this circuit efficiently *approximates* $e_o = -\sum_{j=1}^{j=n} a_j e_j$, where constants $a_j = r_f/r_n$, and e_j vary [5].

For example, in December 2015, the power grid of Ukraine was attacked using targeted malware. The "destructive" malware shut off power to hundreds of thousands of people. This was the first reported cyber-attack to a power grid [1].

Also in 2015, the U.S. Food and Drug Administration issued an advisory that Hospira LifeCare infusion pump systems contained software vulnerabilities. Infusion pump systems are typically used to deliver drugs intravenously, necessitating proper functionality. The Hospira systems were remotely programmable through a health care facility's Ethernet or wireless network. Vulnerabilities could have allowed unauthorized remote control over dosing [2].

Last year, there were also firefighting delays caused by cyber-physical systems; five "hobby drones" interfered with firefighting efforts in Southern California. The disruption forced firefighting aircraft to land because of collision risk with UAVs [3]. UAV regulation is nascent and difficult to

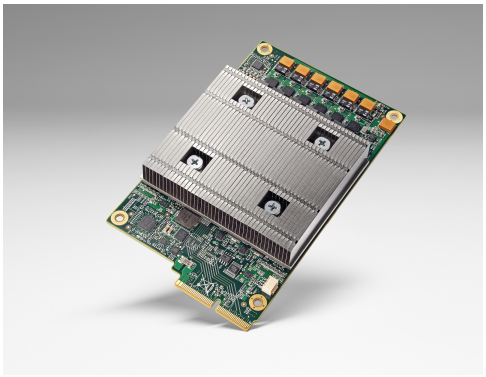

Figure 2. Google's Tensor Processing Unit—an ASIC claimed to "deliver an order of magnitude better-optimized performance per watt for machine learning." [13]

enforce. In the news, we see various ad hoc efforts to control UAV interference, for example, training raptors to take down UAVs, or efforts like Battelle's DroneDefender, which can disrupt UAVs with radio frequency jamming.

One can imagine various, formal, means by which each of the above scenarios may be mitigated. For example, publicly available UAVs could have an emergency override mode, accessible to government operators under some circumstances; drug delivery systems could be mandated to undergo security evaluations by third parties; and power grids and other critical utilities could be put under government control and be heavily defended. Those approaches would most likely result in better systems, but they would not necessarily address the underlying problems related to designing safe and secure CPS from first-principles.

II. Design and Analysis of CPS

The design of safe and secure CPS is more difficult than building "hack-proof" software and hardware (which is a feat in itself). At the root of safe and secure CPS is a need to understand how physics and logic interact in the system of interest. Physical interactions and effects have historically been the domain of mechanical, chemical, industrial, and electrical engineering, as well as physics. Logical interactions have historically been analyzed by computer scientists and mathematicians. Advances in integrated circuit programming abstraction (e.g. microcontrollers and high-level languages) significantly lowers the barrier to entry for building "advanced" CPS. However, the fact that a CPS can perform sophisticated tasks does not imply it is secure or safe.

Understanding the hybrid physical-digital characteristics of CPS is still a developing discipline. The physical aspects of CPS are often *analog* in nature, that is they are systems that take continuous, real-valued inputs from the physical world. The analog aspects of CPS are often most appropriately modeled as systems of differential equations. The digital aspects of CPS are the logic, models, and algorithms implemented within a microprocessor. Hybrid continuous-time/digital theory is unexplored when compared to pure digital (e.g. fundamental computer science) or continuous-time theory; this lack of exploration points towards opportunities for education and research. For a formal introduction to the hybrid theory necessary to approach secure CPS design, see [4] and [6].

III. Applications of Analog Computing in CPS

The necessary inclusion of continuous-time analysis in hybrid CPS modeling hints towards another opportunity: in-situ continuous-time analog computing can be faster, more energy efficient, and more secure than digital solutions in real-time CPS applications.

Until the advent of integrated circuits, electronic analog computing was used. Analog computing elements are excellent at (parallel) summation, integration, and comparison. For the appropriate problems, analog circuits can perform an order of magnitude faster and use an order of magnitude less power than the digital equivalent [7], [8].

For an example analog calculation, consider the dot product performed with the operational amplifier-based circuit in Fig. 1. The circuit *approximates* $e_o = -\sum_{j=1}^{j=n} a_j e_j$, where constants $a_j = r_f/r_n$, and e_j vary. The speed advantage using this circuit is achieved at the node where the currents (denoted as i's in the figure) flow together, summing almost immediately and in parallel. The calculation is performed in parallel thanks to Kirchhoff's Current Law (KCL). "Approximates" is used in the previous sentence, because analog circuits like these introduce noise.

Analog computing has been dominated by digital, but it has never been entirely abandoned. Popular applications currently include mixed-signal integrated circuits—extensively used for signal processing; true random number generation for cryptographic applications; neuromorphic computing, which is the emulation of biological computing models (e.g. neural networks); and statistical computing, also known as computational statistics. In general, applications which can find use in approximate solutions may be good candidates for analog computing.

There are applications for analog computing in CPS. Indeed, if we look at historical analog computing applications, they look surprisingly like CPS: network simulation, power plant development, servo systems, process control, traffic-flow simulation, guidance and control, and craft simulation, to name a few.

With the end of benefits of Moores Law [12], companies and researchers are revisiting applications of non-CPU based computing. From the industrial perspective, standard x86/x64 processors are evidently no longer adequate by themselves; for example, in 2016 Google announced their Tensor Processing Unit for power-optimized machine learning applications [13]; Fig. 2. In December of 2016, Intel

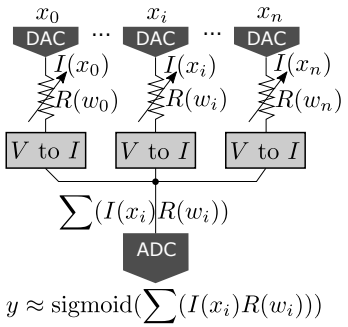

Figure 3. A conceptual analog neuron circuit for sigmoid approximation. Three steps are depicted: scaling inputs by weight ($x_i w_i$), summing the scaled inputs ($\sum x_i w_i$), and applying the sigmoid function. As in Fig. 1, the summation is using KCL [17].

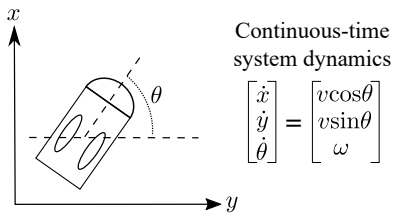

Figure 4. In [15], continuous-time system dynamics of a robot are calculated with an analog circuit. The circuit control implements model-predictive control and tries to minimize energy use. In this figure, ω represents angular velocity, and v represents linear velocity.

announced the acquisition of FPGA manufacturer, Altera; and it appears that this year Xeon CPUs with integrated FPGA coprocessors will ship [14]. Both of these industrial examples are probably all digital. (Google hasn't yet announced the design details of their TPU.) However, the academic community is naturally further on the edge of exploring alternative architectures; consider the following analog computing publications from the past three years.

A. General-Purpose Code Acceleration with Limited-Precision Analog Computation

Researchers from UT Austin, U of Washington, Georgia Tech, and Microsoft made use of the fact that neural networks can be used to approximate any function [17]; Fig. 3. They then integrated an analog neuron circuit with a CPU and accelerated a variety of applications. The analog-accelerated results were then compared to the accelerated results when using an equivalent digital neuron circuit. Average speedup of the analog accelerator was 48% better than digital, and average power consumption was 24% better; however, benefits came with an error cost of ˜10%.

B. Continuous-Time Hybrid Computation with Programmable Nonlinearities

Researchers from Columbia University developed a continuous-time hybrid computer to solve differential equations for control systems [15]; Fig. 4. For an example

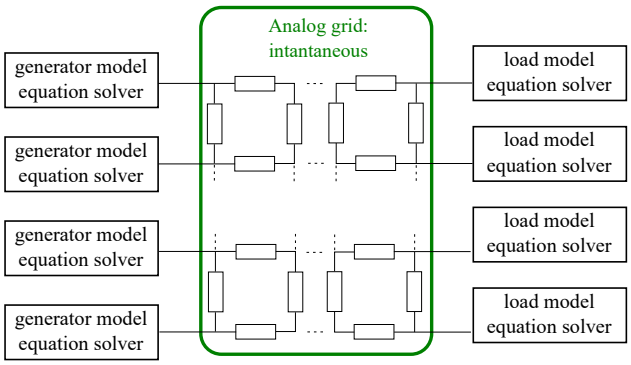

Figure 5. Conceptional view of power grid emulation [18]. Circuit is used to accelerate matrix computations of power system stability analysis, by using instantaneous analog Kirchhoff grid and analog equation solvers. Because of high-speed, low-cost (compared to high-performance numerical simulation), and small size, the system-monitoring devices could be widely distributed throughout a grid.

application, they modeled the system state of a wheeled robot using model-predictive control—this type of control algorithm attempts to predict trajectory while minimizing control effort. In their analog implementation, minimizing control effort is important because power dissipation is dependent on prediction and control activity—if the inputs remain constant, calculations are not performed. When constant inputs are applied to their chip, it predicts the state 0.1s into the future, taking $0.84\mu s$ and using .48nJ. As the researchers point out, this type of systems dynamics simulator has applications in other cyber-physical systems with limited computing energy budgets.

C. High-Speed Power System Transient Stability Simulation Using Highly Dedicated Hardware

Researchers from EPFL built an analog power system emulator for high-speed power system stability analysis [18]; Fig. 5. The system captures details of a power grid, including generators and power lines. Their analog hardware is optimized for simulation time, cost, and size, and it was designed by mapping (and scaling) the components of the real power system to the necessary integral equations; analog circuits were then designed to solve the integral equations in faster-than-real-time.

IV. Safety and Security Benefits of Analog Design in CPS

Analog electronics has always been superior to digital for certain applications, especially when high speed and low power are necessary, and where the output may still be useful even though it contains error. These qualities will leave analog as the only option for resource-constrained CPS; for example, when performing faster-than-real-time cyber-physical system analysis, these devices can be embedded in-situ. In the above section, we saw an application of this in

power systems, but other CPS will benefit, e.g., autonomous vehicles and lightweight military systems.

Another safety benefit to analog is that it is isolated from digital manipulation. Where we see the biggest performance gains with analog is in systems where no analog-to-digital or digital-to-analog conversions are required—such conversions waste time and reduce performance benefits. If a safety-critical CPS subsystem is performed entirely in the analog domain, then the system has insulation from standard network or software-based cyber attacks; in this scenario, an attacker is restricted to physical attacks.

V. Complexities of analog design

While analog computing will provide benefits for certain CPS applications, it is important to enumerate some of the challenges associated with such an approach:

- *Very brittle*: A change in one part of an analog design may require changes to all other parts.
- *Noisy*: Precision limited to $\approx 10^{-4}$.
- *Difficult to build*: Simulation of complex analog circuits is not reliable; must build, test, and tune.
- *Large*: In VLSI, high-performance analog components consume larger area than digital. Analog VLSI technology doubles in components per area every ˜8 years versus ˜2 years (historically) for digital.
- *Suffers from drift*: Temperature will cause analog behavior (and therefore mathematical outputs) to change.

VI. Conclusion

Cyber-physical systems (CPS) are taking increasingly critical roles. Reliable and safe operation of these actuator-based systems have control over many aspects of public health and the economy. The design discipline and engineering education required to properly design, construct, deploy, and maintain (CPS) is immature—this fact is the cause of an expanding list of CPS vulnerabilities and safety incidents. One aspect that will improve reliability of CPS is the inclusion of more sophisticated control and simulation techniques; for many resource-constrained devices this will be impossible, using only digital solutions. Because of its continuous-time, and event-driven nature, analog computing can efficiently solve problems that would otherwise not be possible. In addition, because of isolation from network and software attacks, analog computing could offer protection from current cyber attacks. For some continuous-time resource-constrained applications, where speed maximization, power efficiency, and safety are equally important, hybrid digital-analog solutions will be increasing considered.

References

[1] D. Goodin. "First known hacker-caused power outage signals troubling escalation." Ars Technica, January 4, 2016, Web, April 14, 2016.

[2] "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication." FDA, July 31, 2015, Web, April 15, 2016.

[3] M. Martinez, et al. "Above spectacular wildfire on freeway rises new scourge: drones." CNN, July 19, 2015, Web, April 15, 2016.

[4] E. A. Lee and S. A. Seshia. *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*. Second Edition, http://LeeSeshia.org, ISBN 978-1-312-42740-2, 2015.

[5] J. Smith. *Modern Operational Circuit Design*, John Wiley & Sons, 1971.

[6] P. Marwedel. *Embedded System Design, Embedded Systems Foundations of Cyber-Physical Systems*. Second Edition, Springer, 2015.

[7] S. Shapero, A. S. Charles, C. J. Rozell, and P. Hasler. Low Power Sparse Approximation on Reconfigurable Analog Hardware. IEEE Journal on Emergin and Selected Topics in Circuits and Systems, vol. 2, no. 3, September 2012.

[8] Y. Bai and M. Lin. Energy-Efficient Discrete Signal Processing with Field Programmable Analog Arrays (FPAAs). ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, Monterey, CA, USA, February 2015.

[9] S. M. Koziol. *Reconfigurable Analog Circuits for Autonomous Vehicles*. Ph.D. Dissertation, Georgia Institute of Technology, 2013.

[10] C. Schlottmann. *A Coordinated Approach to Reconfigurable Analog Signal Processing*. Ph.D. Dissertation, Georgia Institute of Technology, 2012.

[11] K. Deems. *High Speed Analog Circuit for Solving Optimization Problems*. Master's Thesis, University of California at Berkeley, 2015.

[12] "The end of Moore's law." The Economist, April 19, 2015, Web, June 1, 2016.

[13] N. Jouppi. "Google supercharges machine learning tasks with TPU custom chip." Google Blog, May 18, 2016, Web, June 2, 2016.

[14] C. Williams. "So you wanna build whopping pools of PCIe flash? Say no more, whisper Intel, Facebook." The Register, March 9, 2016, Web, June 2, 2016.

[15] N. Guo, et al. Continuous-time hybrid computation with programmable nonlinearities. European Solid-State Circuits Conference (ESSCIRC), 2015.

[16] S. Vichik and F. Borrelli. Solving linear and quadratic programs with an analog circuit. Computers & Chemical Engineering 70 (2014): 160-171.

[17] R. Amant, et al. General-purpose code acceleration with limited-precision analog computation. ACM SIGARCH Computer Architecture News 42.3 (2014): 505-516.

[18] I. Nagel, et al. High-Speed Power System Transient Stability Simulation Using Highly Dedicated Hardware. Power Systems, IEEE Transactions on 28.4 (2013): 4218-4227.