

Resiliency in Cyber-Physical Systems

Oleg Sokolsky, University of Pennsylvania

Nicola Bezzo, University of Virginia

In living species, it is often the resilience of an organism that determines its long-term success and phylogenesis. In computing, cyber-physical systems are also only as good as their level of resilience.

Modern cyber-physical systems (CPSs) feature a tight integration of physical, computation, and communication processes.¹ In CPSs, computers, networks, and sensors work in synergy to control complex operations systems using feedback loops. In the last decade, there has been a rapid growth of research into the deployment of CPSs in areas such as automation, energy, security, healthcare, manufacturing, transportation, and infrastructure design. Some examples of CPSs include industrial systems, sensor networks, medical devices, smart buildings, and autonomous and robotic systems. Because the physical processes in these systems affect computations and vice versa, there has been a growing realization that a new set of design principles, tools, and techniques is needed to effectively design and implement these systems.

CPSs are often safety- and life-critical and operate in unpredictable and possibly hostile environments. While, on one hand, the interaction between computation and physical components has enabled the development of highly automated and precise CPSs, it is also creating safety and security concerns. CPSs must maintain their operations despite dramatic changes in their environments and are likely to encounter events that can interfere with their operation. They need to tolerate a variety of component failures, including new kinds of failures that result from unplanned interactions between physical and computational parts of the system. In addition, the tight integration between physical and computational parts of the system gives rise to

new kinds of malicious attacks. In fact, these systems are typically not built with security in mind, and attackers can compromise or take over portions of the entire system. Hence, it is necessary to build CPSs to be resilient against such adverse events.

RESILIENCY IN CPSs

We adapt the definition of *resiliency* from a report by the National Academies of Sciences,² which defines it as “a system’s ability to anticipate, resist, recover from, and reconfigure after adverse events, such as cyberattacks, failures, and disturbances.” To ensure resiliency, we need multidisciplinary approaches that provide state awareness, intelligence, control, safety, security, effective human–system interaction, robust communications, and reliable computation and operation.

To achieve resiliency, it is necessary to design a system considering a wider range of scenarios, conditions, and threats. Resilient approaches can be designed as 1) *reactive*, that is, concerned with detecting, tolerating, and correcting a problem; 2) *proactive*, that is, concerned with preventing problems from happening in the first place; or 3) *hybrid*, that is, concerned with preventing problems when possible and reacting to all other situations.

Often, the only available possibility is to redesign or retrofit an existing system’s architecture to accommodate resiliency and guarantee safety. If this weren’t already difficult enough, to further complicate this problem, adding resiliency to systems that were not designed for it can be challenging because of their very limited resources. Thus, this operation may

be possible only in limited cases, and it may often come at the expense of the system’s performance.

Among all of the events that a system may encounter during its life, security is one of its main concerns because the nature of an attack may be stealthy and thus hard to detect using traditional fault-detection methods.

This issue of *Computer* addresses the applications, architectures, and development methodologies as well as the safety, security, and reliability approaches necessary to enable CPS resiliency. Special emphasis is given to security and failure problems, which are the foremost concerns when designing and analyzing safety critical systems.

IN THIS ISSUE

CPS security has been investigated in automotive, power distribution, and industrial settings by many researchers over the last few years; however, this is a concern for many other applications, as demonstrated by the articles in this issue that deal with the Internet of Things, power grids, aerial vehicles, and train control systems.

To reason about the resiliency of a system, we need to be able to specify what properties of the system are critical to be preserved. Then, relying on detailed fault and attack models, we should be able to analyze the architecture of the system and provide guarantees that these properties will be achieved. In “A Formal Approach to Constructing Secure Air Vehicle Software,” Darren Cofer, Andrew Gacek, John Backes, Michael W. Whalen, Lee Pike, Adam Foltzer, Michal Podhradsky, Gerwin Klein, Ihor Kuz, June Andronick, Gernot Heiser, and Douglas Stuart describe such a framework rooted

ABOUT THE AUTHORS

OLEG SOKOLSKY is a research professor of computer and information science at the University of Pennsylvania. His research focuses on various aspects of cyber-physical systems, including model-based designs, cyber-physical security, and safety and timing analysis. Sokolsky received a PhD from Stony Brook University. Contact him at sokolsky@cis.upenn.edu.

NICOLA BEZZO is an assistant professor of systems and information engineering and electrical and computer engineering at the University of Virginia. His research focuses on assured and resilient planning and control of autonomous robotic systems including runtime monitoring, planning, and control of autonomous mobile robots, heterogeneous robotic systems, and cyber-physical security. Bezzo received a PhD from the University of New Mexico. Contact him at nbezzo@virginia.edu.

in formal methods, which is an important step toward achieving “resiliency by construction.”

The challenges associated with ensuring the resiliency of a system grow dramatically with the scale of the system. The problem becomes even more difficult in dynamic, adversarial environments, where the nature of threats is hard to predict. In “Toward an Internet of Battlefield Things: A Resilience Perspective,” Tarek Abdelzaher and a large multidisciplinary team of researchers lay out a vision for addressing such a challenge in the context of a research initiative recently begun by the US Army.


Although several attack-resilient techniques have been identified in the last few years, solving this problem is essentially impossible because new attack vectors requiring new defense mechanisms continue to be discovered. With these considerations in mind, the article “Cyberattacks on Primary Frequency

Response Mechanisms in Power Grids” by Varun Badrinath Krishna, Ziping Wu, Vaidehi V. Ambardekar, Richard Macwan, and William H. Sanders presents an illustrative example of a recently discovered cyber-physical attack on power grids and discusses defenses against it. Power grids present a particularly insightful case study of cyber-physical security because the availability of electric power is critical to the functioning of our society, and a wide variety of attack vectors has been discovered and studied by our industry for a number of years.

Many approaches that establish a system’s resiliency are architectural in nature. A major design challenge is to introduce components into the system that detect faults and attacks and manage the process of adaptation without making these components points of failure themselves. In “An Attack-Resilient CPS Architecture for Hierarchical Control: A Case Study

on Train Control Systems,” Yuchang Won, Buyeon Yu, Jaegeun Park, In-Hee Park, Haegeun Jeong, Jeanseong Baik, Kyungtae Kang, Insup Lee, Sang Hyuk Son, Kyung-Joon Park, and Yongsoo Eun propose such an architecture for hierarchical control systems and illustrate its instantiation in a system for coordinating train traffic.

Much attention has been given to resiliency against malicious attacks; however, resiliency to faults is just as important for safety-critical CPSs. Compared to traditional fault-tolerance techniques, resiliency-based approaches emphasize adaptation to unknown or unexpected faults. In “Contract-Based Hierarchical Resilience Management for Cyber-Physical Systems,” Mohammad Shihabul Haque, Daniel Jun Xian Ng, Arvind Easwaran, and Karthikeyan Thangamariappan offer a hierarchical fault-management framework that relies on component contracts to detect and mitigate faults.

The articles in this issue provide complementary perspectives on the problem of CPS resiliency. Despite much work in recent years, we are just scratching the surface of this area. We expect that the scope and importance of this problem will keep growing as CPSs become more and more autonomous and continue to influence aspects of our lives. 

REFERENCES

1. M. Wolf, “Computing in the real world is the grandest of challenges,” *Computer*, vol. 51, no. 5, pp. 90–91, 2018.
2. The National Research Council, *Disaster Resilience: A National Imperative*. The National Academies Press, 2012.