Safety and Security of Cyber–Physical and Internet-of-Things Systems

By MARILYN WOLF
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA

DIMITRIOS SERPANOS
Electrical & Computer Engineering, University of Patras, Patras GR-26504, Greece

Computer system security and engineering system safety have traditionally been very distinct topics pursued by people with very different expertise. The advent of cyber–physical systems and the Internet-of-Things (IoT) changes that dynamic. Safety and security are now inextricably linked through our linkage of computer hardware and software with complex physical plants. Computers have been added to traditional engineering systems to achieve goals that we cannot achieve using traditional mechanical control. The automobile provides an important early example of the benefits of cyber–physical systems: computer engine control allowed manufacturers to simultaneously meet stiff requirements on both fuel economy and emissions; features such as antilock brakes and traction control improved vehicle handling and safety; and a new generation of supercars use software to not only provide sophisticated vehicle capabilities but also to change the vehicle's handling characteristics at the push of a button.

Ensuring that cyber–physical and IoT systems are safe, secure, reliable, and private will require not only the consistent application of current best practices (something that does not always happen) but the development of new design methodologies and architectures. Safety and security concerns both influence each other. On the one hand, the physical systems connected to computer systems create a larger attack surface than is the case for a pure computer system. Physical plants provide side channels that allow attackers to both observe and manipulate the computer system. On the other hand, safety concerns magnify the consequences of many traditional security attacks. One example which illustrates the interaction between safety and security occurred in May 2015 when a person claimed to have hacked into the flight control systems of a Boeing 737 operated by United Airlines while the aircraft was in flight [5]. The person claimed to have been able to enter into the flight control systems through the onboard entertainment system with sufficient authority to issue a command to the flight controls.

The stakes for safety and security are high in part because of the long service life of these systems. Computer systems practitioners have long relied on Moore's Law to obsolesce computers quickly, in contrast to the emphasis on

Digital Object Identifier: 10.1109/JPROC.2017.2699401

long-lived systems in many engineering disciplines. However, many cyber–physical systems have service lives measured in decades. IoT devices that are installed or embedded into industrial control systems or smart city networks will have much longer lifespans than the consumer electronics devices that industry is used to producing.

What sorts of new approaches will be needed? Clearly, both design-time and runtime methods must be used. Both safety and security are used to combining design-time methods with runtime checks on the operation of both the physical plant and the computer system. The threats from Internet-enabled cyber–physical systems make runtime methods particularly important. New threats may emerge from the Internet which the system was not designed to handle. We need to be able to monitor the system during operation for threats. We also need to be able to update the system after deployment to handle those emerging threats.

Many designers of both software and hardware will need to make more consistent use of specification-driven design methodologies. For example, the DO-178C standard for aviation systems requires that both software and the tools used to design that software must undergo qualification processes. In contrast, many IoT devices are designed using much looser methodologies and tool sets derived from consumer electronics. Code synthesis and the use of certified libraries can improve security and safety; ultimately, that approach should improve design productivity as well.

Modeling cyber–physical and IoT systems is much harder than is the case for traditional computer systems. Computer system designers rely on abstraction to hide detail and composition to construct large systems. Nonlinear systems, however, are not composable in the traditional computer science sense. Model-based design has made progress in the verification composable and synthesis of nonlinear cyber–physical systems. However, more work needs to be done to provide security analysis for systems with nonlinear plants.

Threats may come from within the design process as well as from without. Software bugs can result in operational errors of the physical plant. A buffer overflow problem caused the Planetary Society to temporarily lose contact with its spacecraft [2]. Software problems in the fuel system of an Airbus A400M were implicated in a crash that killed four people [4].

Beyond inadvertent errors, malicious operators may insert Trojans in either hardware or software. Many cyber–physical and IoT systems are systems-of-systems that rely on complex subsystems provided by outside entities. Dieselgate, the program by Volkswagen management to install defeats for required emission control software [1], is a very public illustration that systems may not live up to their claimed specifications. We may see third-party monitors for certain types of systems that provide independent analysis and auditing of cyber–physical systems as they operate.

Agencies and regulatory bodies understand the importance of security for safety-critical systems. The U.S. National Highway Traffic Safety Administration published a set of cybersecurity best practice guidelines for vehicles [7]. The U.S. National Institute of Standards and Technology published a set of guidelines for smart grid cybersecurity. The European Union Agency for Network and Information Security published a report which called for standards for smart grid security certification that would follow smart grid devices from their design to decommission.

Safety and security will require computer system designers to become much more like traditional engineers. Similarly, every engineer will need to be familiar with computer security concepts such as digital signatures and root-of-trust. The required techniques will require time to develop and implement. But along the way, we must strive to minimize long-term problems and avoid baking-in poor design decisions. ■

REFERENCES

[1] C. Davenport and J. Ewing, "VW is said to cheat on diesel emissions; U.S. to order big recall," *The New York Times*, vol. 18, Sep. 2015. [Online]. Available: http://www.nytimes.com/2015/09/19/business/volkswagenis- ordered-to-recall-nearly-500000-vehicles-over-emissionssoftware.html?smid=tw-nytimes&smtyp=cur&_r=0

[2] J. Davis, "Software glitch pauses LightSail test mission," *Planetary Soc.*, vol. 26, May 2015. [Online]. Available: http://www.planetary.org/blogs/jason-davis/2015/20150526-software-glitch-pauses-ls-test.html

[3] *Smart Grid Security Certification in Europe: Challenges and Recommendations*, European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2014.

[4] J. Flottau and T. Osborne, "Software cut off fuel supply in stricken A400M," *Aviation Week*, vol. 19, May 2015. [Online]. Available: http://aviationweek.com/defense/software-cut-fuel-supply-stricken-a400m

[5] E. Perez, "FBI: Hacker claimed to have taken over flight's engine controls," *CNN*, May 2015. [Online]. Available: http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html

[6] *Guidelines for Smart Grid Cybersecurity: Volume 1—Smart Grid Cybersecurity Strategy, Architecture, and High–Level Requirements* National Institute Standards Technology, Gaithersburg, MD, USA, Sep. 2014.

[7] "Cybersecurity best practices for modern vehicles," National Highway Traffic Safety Administration, Washington, Tech. Rep. DOT HS 812 333, Oct. 2016.