

Insights on the Security and Dependability of Industrial Control Systems

Frank Kargl and Rens W. van der Heijden | University of Ulm
Hartmut König | Brandenburg University of Technology Cottbus
Alfonso Valdes | University of Illinois at Urbana-Champaign
Marc C. Dacier | Qatar Computing Research Institute

Industrial control systems (ICSs) allow for significant automation of industrial processes, improving their efficiency and reducing their cost. The trend toward the use of commodity hardware and software in networked distributed control systems (DCSs) over the past few decades has furthered this development, allowing a centralization of monitoring and more control over distributed production processes. However, connecting ICSs brings new security and safety issues.

The past few years have highlighted the fact that many critical infrastructures are vulnerable, especially to targeted attacks carried out by resourceful and motivated attackers. ICS malfunctions can cause huge economic losses and even endanger human lives. The Stuxnet malware¹ that damaged approximately 1,000 Uranium centrifuges in the Iranian

enrichment facility in Natanz is the most widely reported example of an attack impacting an ICS, but many similar examples have been published. The proliferation of sophisticated Stuxnet-like malware (such as Duqu, Flame, and Gauss) shows the imminence of the threat and the limitations of our detection and response countermeasures.

Challenges in Industrial Control Systems

Due to the often proprietary nature of ICSs, missing documentation, and lack of access to standards, the security community has only recently started to turn its attention to ICSs. Traditionally, the focus of ICSs has been on safety: each system has a fail-safe that halts the process if something goes wrong. However, safety mechanisms typically weren't designed to withstand dedicated attacks. An additional challenge

arises with ICSs' high costs and mission criticality. This leads to very long lifetimes—machines from the 1980s are not uncommon—as well as complex warranty and service contracts. Such contracts guarantee the safety of a particular system configuration, often requiring specific software versions that were explicitly tested. This causes a massive security management issue—upgrading or patching systems often isn't possible, as it would violate the contract and could lead to system failure. Thus, updating ICS requires extensive and lengthy testing procedures, which prevents quick reactions to discovered vulnerabilities. Similarly, replacing legacy systems often isn't an option.

The shift to more standardized systems using Internet protocols or commodity operating systems has led to significant cost savings. However, it's becoming clear that more homogeneous systems simplify attacks. By networking ICSs into cyber-physical systems (CPSs), two very different cultures of system design intersect: control engineering, where random effects in a physical process mandate stringent safety mechanisms, and computer networking, where developers are accustomed to malicious attackers and include security mechanisms in the design.

Other relevant research trends include "Industry 4.0,"² which addresses more flexible and personalized manufacturing processes based on smarter sensors, actuators, and control, and smart grids that will revolutionize the way electricity is generated, disseminated, and consumed.

Both the existing state of ICS security and the upcoming trends

give rise to new research challenges, which were discussed during a recent research seminar at Dagstuhl, a computer science research center in Germany. The Dagstuhl seminars bring together industry and academia experts from all over the world. The main objective of the 2014 seminar was to discuss ideas about how to detect advanced attacks on ICSs and how to limit their impact on the physical components. This is closely related to the question of whether and how reactive security mechanisms like intrusion detection systems (IDSs) can be tailored to ICSs and the processes they control. To some extent, adopting existing security approaches from other areas (such as conventional networks, embedded systems, sensor networks, and robotics) seems possible, but it remains to be seen whether this is sufficient due to the differences in desired security level for ICSs compared to these areas. In some cases, it might be necessary to design security mechanisms specifically for ICSs.

Discussion Results and Research Challenges

Based on the discussions at the Dagstuhl seminar,³ we aim to provide an overview of the most important research challenges agreed upon by the participants.

Process Awareness

One prominent but controversial idea is to integrate specific knowledge about the process that an ICS controls into an IDS that monitors the network. IDSs are a promising tool for engineers to maintain the security of a traditional network, and many have been proposed specifically for networked ICSs. By including semantic knowledge about the controlled process in IDS design, security researchers aim to improve detection accuracy. According to this idea, attacks

would lead to inconsistent or implausible sensor or control data being communicated in the network. However, both safety and security researchers have pointed out that process-aware IDSs would essentially duplicate the work done by the ICSs: monitoring the process as it's executed. They argue that duplication isn't only a waste of resources but could also be counterproductive because, unlike IDS, safety systems are extensively tested and carefully designed. If these systems differ, it's unclear which should be trusted.

Toward Dependability

The interaction between safety and security mechanisms is an important aspect and requires further analysis. These issues are currently treated separately, but we think researchers and practitioners in both areas should work together to develop unified mechanisms. This would include a tighter integration of security mechanisms with control loops, which form the core of ICS. This would also require security mechanisms that can guarantee availability—an issue that's often neglected.

Last Line of Defense

Although ICSs are often associated with critical infrastructures such as nuclear plants, even those that are less critical (such as manufacturing plants) require a last line of defense. These types of monitoring and safety mechanisms shouldn't be connected or coupled with a potentially attackable ICS; they should provide a ground truth for operators and prevent the system from entering clearly forbidden states.

Incident Response

Determining the correct response to a security incident is a neglected and often difficult issue. In many situations, a sudden shutdown or disconnection, which might be

applied in normal IT security, isn't a viable option. Intrusion detection and prevention systems should be able to provide a flexible reaction to detected security breaches to allow a form of "graceful degradation." This approach is similar to that of safety mechanisms: an ICS should enter a more robust and fail-safe state when an attack is detected, perhaps to the detriment of the controlled process's efficiency and output. However, this reaction might also be a potential attack vector, if this is the attacker's goal.

The Importance of User Interfaces

More attention should be paid to security mechanisms' user interfaces to provide operators and security experts with appropriate options for analysis and reaction if attacks cause critical situations. This is especially important when considering attacks that attempt to trigger security responses to reduce the efficiency of the controlled process. In support of this goal, security systems should provide more fine-grained output. This could allow operators to distinguish between disruptive and destructive attacks and take appropriate countermeasures, and it would also allow for better forensics.

The Industry–Academia Gap

In ICS security, a huge gap exists between academia and industrial practice. While research targets highly sophisticated attacks and countermeasures, many real-world deployments fail due to a lack of the simplest security best practices. Closing this gap will require a huge effort that should start with identifying which best practices must be applied and which don't fit in ICSs. This analysis should explicitly include safety constraints in its scope, as these constraints are often one of the reasons existing best practices aren't applied.

Security Management

In security and risk management, ICSs also pose big challenges, partly due to the huge scale of some installations. In addition, the lack of a realistic attacker model that is required to find the right level of security and perform a proper risk assessment is a significant challenge. Because good risk assessments aren't always available, the economic pressure to build cost-effective security solutions is often insufficient.

Diversity and Redundancy

Diversity and redundancy are generally good for ICS security because they significantly increase the cost for an attacker to design attacks and malware that work for multiple ICSs. On the other hand, operating a very diverse installation complicates good security management. So it's still unclear whether ICSs' migration to a small number of vendors and standards (in terms of protocols and operating systems) will provide more benefits to attackers or defenders. This shift is most likely an irreversible one, due to the significant cost savings and increased efficiency and interoperability it provides.

Reliable and Secure Update Processes

The fact that ICSs are often very long-lived installations and that the duration of innovation cycles in ICSs is very different from those in information and communication technology (ICT) creates huge problems for maintaining ICS security. Well-defined, certified update processes that are guaranteed for the lifetime of an ICS would significantly increase security. It's likely that the embedded systems in field devices will undergo several generations of firmware before the device is retired from service. However,

secure access to the device, firmware authentication, and assurance that an update won't have adverse consequences are more difficult to attain in ICSs than in conventional networks and computer systems. Moreover, control applications are typically developed for commodity platforms, for which the OS vendor will issue periodic patches and updates. Currently, an ICS vendor typically verifies patches before recommending that customers install

field location. With the increasing adoption of distributed embedded systems in the field and wireless communications, new challenges are arising when it comes to separating systems into zones.

While research targets highly sophisticated attacks and countermeasures, many real-world deployments fail due to a lack of the simplest security best practices.

them. Customers have to wait for a planned system maintenance interval to apply the updates, because availability is arguably more critical. These factors extend the window of vulnerability available to attackers.

Separation and Isolation

Despite evidence that sophisticated malware can break air gaps, isolation mechanisms such as air gaps, virtualization, sandboxes, and VPNs are among the most effective security mechanisms for ICSs.

With the introduction of computerized controls in industrial processes that are as diverse as manufacturing, energy production, and delivery, several best-practice system architectures have emerged that rely on isolation. These generally separate enterprise and process zones via a demilitarized zone with firewalls in between.⁴ The process zone might be segmented into a control zone and a field zone.

These architectural models are possible where all the systems are connected by wires and where a physical security perimeter provides additional protection, even if it's only a locked cabinet at a

ICS is a very broad term that encompasses many extremely heterogeneous types of systems, which vary widely in application, spatial footprint (from the manufacturing plant to a multinational electric grid), system requirements for monitoring and control, time scale, connection topology, impact of a potential compromise, and other factors. Participants in the Dagstuhl workshop agreed

that the security challenges that need to be addressed are often very similar, so there can be meaningful progress in ICS security in general. Systems in manufacturing, refining, and power grids have similarities: some protocols are used in diverse ICS environments, and system vendors often supply multiple sectors.

Addressing security challenges that are common to the broad class of ICSs is the low-hanging fruit that the research and security community should address in the short term. However, we're already seeing a migration in many sectors from a relatively small number of devices with embedded system controls that are connected through physical wires to a larger number of widely distributed, inexpensive sensor networks and controls that frequently communicate through wireless networks. While security principles might still apply generically, a certain degree of specialization in security solutions appears unavoidable. ■

Acknowledgments

We thank the Dagstuhl Seminar 14292 participants, whose expertise and con-

tributions to the seminar provided the basis for this article.

References

1. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, vol. 9, no. 3, 2011, pp. 49–51.
2. N. Jazdi, "Cyber Physical Systems in the Context of Industry 4.0," *IEEE Int'l Conf. Automation, Quality and Testing, Robotics (AQTR 14)*, 2014, pp. 1–4.
3. "Network Attack Detection and Defense: Securing Industrial Control Systems for Critical Infrastructures," Dagstuhl Seminar 14292, July 2014; www.dagstuhl.de/de/programm/kalender/semhp/?seminr=14292.
4. Cisco Systems, "Converged Plant-

wide Ethernet Solution," *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*, 2011; www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html.

Frank Kargl is a full-time professor at the University of Ulm and chairs the Institute of Distributed Systems. Contact him at frank.kargl@uni-ulm.de.


Rens W. van der Heijden is a PhD candidate in the Institute of Distributed Systems at the University of Ulm. Contact him at rens.vanderheijden@uni-ulm.de.

Hartmut König is a full-time professor at the Brandenburg University

of Technology Cottbus and chair of Computer Network and Communication Systems. Contact him at koenig@informatik.tu-cottbus.de.

Alfonso Valdes is the managing director of Smart Grid Technologies at the University of Illinois at Urbana-Champaign. Contact him at avaldes@illinois.edu.

Marc C. Dacier is a principal scientist of cybersecurity at Qatar Computing Research Institute. Contact him at marc.c.dacier@gmail.com.

 Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



KEEP YOUR COPY OF IEEE SOFTWARE FOR YOURSELF!

Give subscriptions to your colleagues or as graduation or promotion gifts—way better than a tie!

IEEE Software is the authority on translating software theory into practice.

www.computer.org/software/subscribe

SUBSCRIBE TODAY