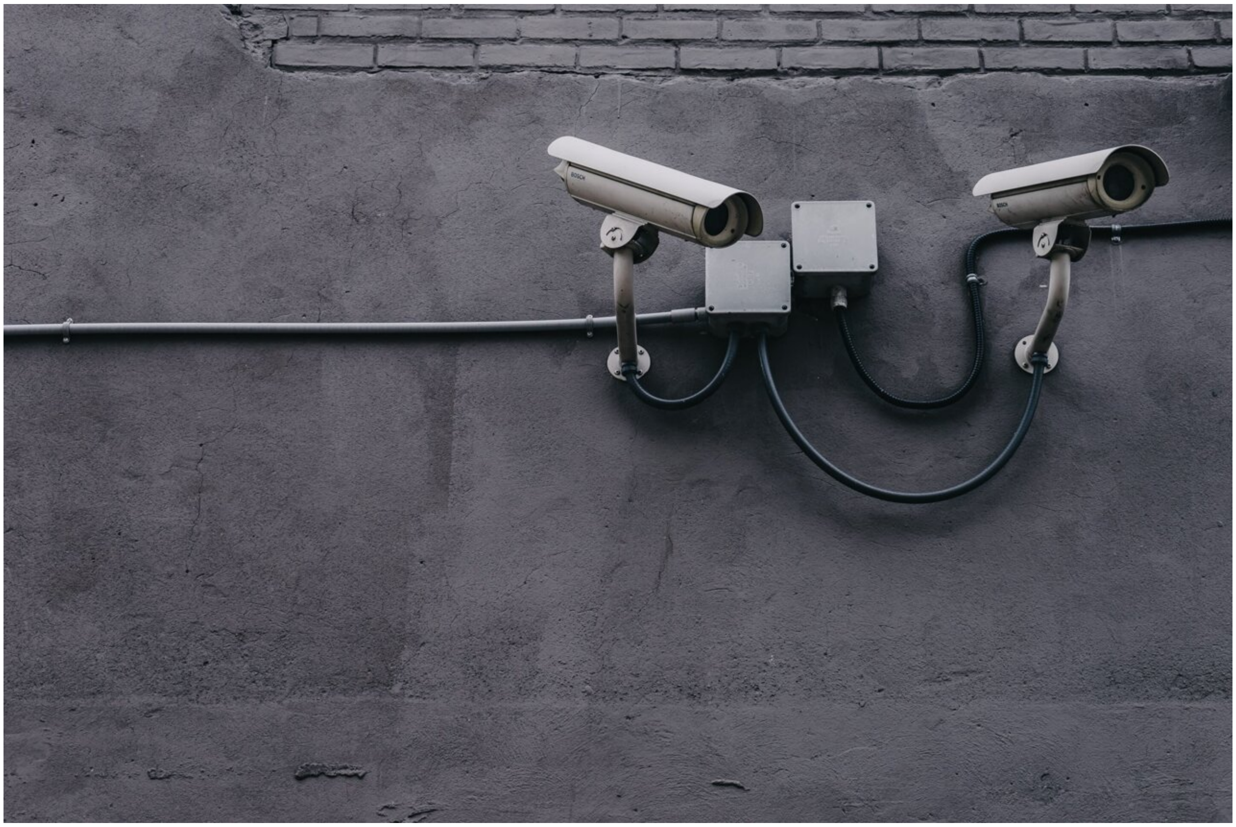
Final version of industrial control systems security guide published

June 22 2011



Credit: Unsplash/CC0 Public Domain

The National Institute of Standards and Technology (NIST) has issued the final version of its Guide to Industrial Control Systems (ICS) Security (SP 800-82),* intended to help pipeline operators, power producers, manufacturers, air traffic control centers and other managers of critical infrastructures to secure their systems while addressing their unique performance, reliability, and safety requirements.

Finalized after three rounds of public review and comment, the guide is directed specifically to federally owned or operated industrial control systems (ICS), including those run by private contractors on behalf of the federal government. Examples include the mail handling operations, air traffic control towers, and some electricity generation and transmission facilities and weather observation systems. However, the guide's potential audience is far larger and more diverse than the federal government, since about 90 percent of the nation's critical infrastructure is privately owned.

The guide responds to responsibilities assigned to NIST under the Federal Information Security Management Act (FISMA). The law directs NIST to develop information security standards and guidelines for non-national security federal information systems. While these FISMA-related specifications are not mandatory for the private sector or state and local governments, many businesses and other organizations have adopted the NIST-developed standards and guidelines. Drafts of the new document have been downloaded more than 1,000,000 times, and the guide already is referenced in industry-specific security publications.

Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems and programmable logic controllers. The scope of facilities and equipment encompassed by these technologies range from broadly dispersed operations, such as natural gas pipelines and water distribution systems, down to individual machines and processes.

Most industrial control systems began as proprietary, stand-alone systems that were separated from the rest of the world and isolated from most external threats. Today, widely available software applications, Internet-enabled devices and other nonproprietary IT offerings have been integrated into most such systems. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems to malicious attacks, equipment failures and other threats.

As a rule, these systems must operate continuously and reliably, often around the clock. Unlike information technology (IT) systems, which process, store, and transmit digital data, industrial control systems typically monitor the system environment and control physical objects and devices, such as pipeline valves. Disruptions or failures can result in death or injury, property damage, and loss of critical services.

Due to these unique performance, reliability and safety requirements, securing industrial control systems often requires adaptations and extensions to the NIST-developed security standards and guidelines for IT systems only. The new guide describes these adaptations and extensions, provides an overview of various systems and their organizational layouts, describes typical threats and vulnerabilities, and recommends appropriate countermeasures.

"Securing an industrial control system requires a proactive, collaborative effort that engages cyber security experts, control engineers and operators and other experts and experienced workers," says NIST mechanical engineer and lead author Keith Stouffer. "It also requires factoring in—and addressing—new risks introduced by the evolving 'smart' electric power grid."

Stouffer recommends using the new guide along with Guidelines for Smart Grid Cyber Security (NISTIR 7628), which NIST issued last September, to tackle security issues arising from the convergence of the electric power Smart Grid and ICS.

The free 155-page guide can be downloaded from the NIST Computer Security Resource Center at: csrc.nist.gov/index.html

More information: *K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security (SP 800-82). June 2011.

Provided by National Institute of Standards and Technology

Citation: Final version of industrial control systems security guide published (2011, June 22) retrieved 26 April 2024 from https://phys.org/news/2011-06-version-industrial-published.html