

# Vulnerabilities give hackers ability to open prison cells from afar

By [Sean Gallagher](#) | Published 7 minutes ago

Researchers have demonstrated a vulnerability in the computer systems used to control facilities at federal prisons that could allow an outsider to remotely take them over, doing everything from opening and overloading cell door mechanisms to shutting down internal communications systems. Tiffany Rad, Teague Newman, and John Strauchs, who presented their research on October 26 at the [Hacker Halted](#) information security conference in Miami, worked in Newman's basement to develop the attacks that could take control of prisons' industrial control systems and programmable logic controllers. They spent less than \$2,500 and had no previous experience in dealing with those technologies.

The [Washington Times](#)' [Shaun Waterman reports](#) that the researchers had delivered their findings to state and federal prison authorities, and that the Department of Homeland Security had independently confirmed their research. "We validated the researchers' initial assertion ... that they could remotely reprogram and manipulate [the ICS software and controllers]," Former National Cybersecurity and Communications Integration Center director Sean P. McGurk, who left DHS in September, told the *Washington Times*.

The researchers began their work after Strauchs was called in by a warden to investigate an incident in which all the cell doors on one prison's death row spontaneously opened. While the computers that are used for the system control and data acquisition (SCADA) systems that control prison doors and other systems in theory should not be connected to the Internet, the researchers found that there was an Internet connection associated with every prison system they surveyed. In some cases, prison staff used the same computers to browse the Internet; in others, the companies that had installed the software had put connections in place to do remote maintenance on the systems. But even in the absence of an Internet connection, the researchers found, a [Stuxnet-like attack](#) could be brought in on a flash drive and introduced into the network, either through social engineering or through the actions of a bribed guard or other prison employee.

"You could open every cell door, and the system would be telling the control room they are all closed," Strauchs, a former CIA operations officer, told the *Times*. He said that he thought the greatest threat was that the system would be used to create the conditions needed for the assassination of a target prisoner.