



CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

Highlights of [GAO-04-628T](#), a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

Why GAO Did This Study

Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines. In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. At the request of the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, this testimony will discuss GAO's March 2004 report on potential cyber vulnerabilities, focusing on (1) significant cybersecurity risks associated with control systems (2) potential and reported cyber attacks against these systems (3) key challenges to securing control systems, and (4) efforts to strengthen the cybersecurity of control systems.

What GAO Recommends

In a March 2004 report, GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with GAO's recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-04-628T.

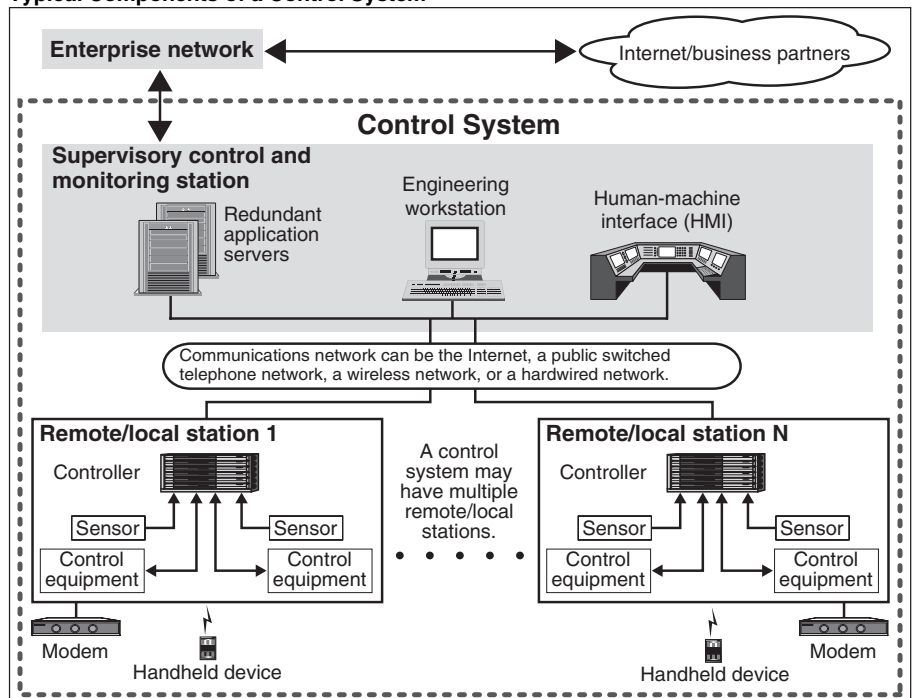
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyrf@gao.gov.

What GAO Found

In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems. Typical control system components are illustrated in the graphic below. Control systems can be vulnerable to a variety of attacks, examples of which have already occurred. Successful attacks on control systems could have devastating consequences, such as endangering public health and safety.

Securing control systems poses significant challenges, including limited specialized security technologies and lack of economic justification. The government, academia, and private industry have initiated efforts to strengthen the cybersecurity of control systems. The President's *National Strategy to Secure Cyberspace* establishes a role for DHS to coordinate with these entities to improve the cybersecurity of control systems. While some coordination is occurring, DHS's coordination of these efforts could accelerate the development and implementation of more secure systems. Without effective coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

Typical Components of a Control System



Source: GAO (analysis), Art Explosion (clipart).