October 1, 2003

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Securing Control Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-140T, 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 the electric power industry, they can monitor and control the current and voltage of electricity through relays and circuit breakers; and in water treatment facilities, they can monitor and adjust water levels, pressure, and chemicals used for purification.

In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. The House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census asked GAO to testify on potential cyber vulnerabilities.

GAO's testimony focused 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) steps that can be taken to strengthen the security of control systems, including current federal and private-sector initiatives.

www.gao.gov/cgi-bin/getrpt?GAO-04-140T.

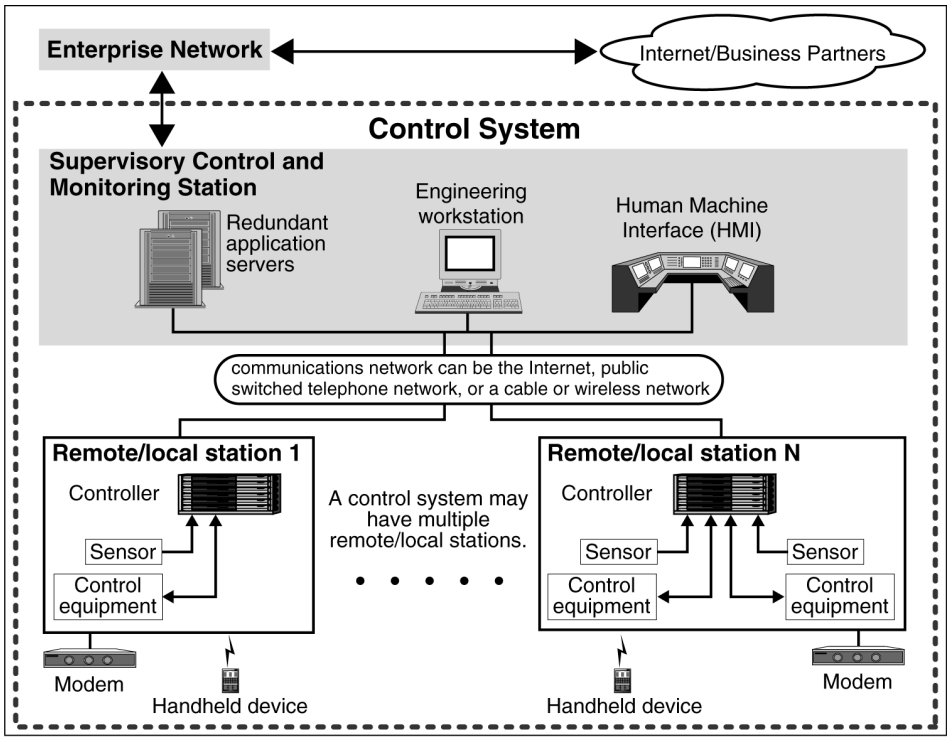
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

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, the increased connectivity of control systems to other systems, constraints on the use of existing security technologies for control systems, and the wealth of information about them that is publicly available. Common 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; damaging the environment; or causing a loss of production, generation, or distribution of public utilities.

Securing control systems poses significant challenges, including technical limitations, perceived lack of economic justification, and conflicting organizational priorities. However, several steps can be taken now and in the future to promote better security in control systems, such as implementing effective security management programs and researching and developing new technologies. The government and private industry have initiated several efforts intended to improve the security of control systems.



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