



# Mississippi State University



## Minimal Trustworthy Computing Base (TCB) for SCADA Security

Dr. Mahalingam Ramkumar, ramkumar@cse.msstate.edu, 662-325-8435

Prevent, Protect, Respond, Recover

### Homeland Security Challenge:

Attacks on Supervisory Control and Data Acquisition (SCADA) systems can take several forms. Security loopholes that can now be exploited by attackers to gain control of the supervisory system include defects in the SCADA software, weaknesses of the underlying operating system, and even untrusted hardware in general purpose computers. SCADA systems were never meant to be accessed by the public, but many are now controlled via the Internet, leaving them vulnerable to infiltration and attack.

### Research Project Solution:

This project is intended to examine substantially different approaches to securing SCADA systems, and to use those results to architect a practical low-cost solution for protecting the integrity of SCADA systems that control critical infrastructures. Results shall include a minimal trustworthy computing base (TCB) for SCADA systems. A trustworthy computing base is defined as a set of guaranteed functionality which, as assumed, cannot be modified. This effort will focus on SCADA systems used for an electric power grid and a municipal water supply system. The effort will also include collaborations with operational end-users and vendors.

### National Implications:

Cyberterrorism is a growing threat to critical infrastructure protection and the nation's economy. There are reports of systems that can infiltrate and compromise water, transportation, and power infrastructures. Intelligence reports show there are terrorist computer systems with details about supervisory control and data acquisition (SCADA) systems in America. These systems control critical infrastructure, including electrical grids, nuclear plants, fiber-optic cables, oil and gas pipelines, dams, railroads and water storage and distribution facilities. The results of this research should help protect critical infrastructure against malicious cyber attacks.



SCADA Control Systems Laboratory at Mississippi State University (MSU)



Mississippi River Dam.

[www.serri.org](http://www.serri.org)

For More Information on SERRI, contact;

Warren Edwards, Director, SERRI  
865-574-8277, edwardswc@ornl.gov

Ben Thomas, Operations Manager  
865-574-5438, thomasbjr@ornl.gov

SERRI is managed by the Department of Energy's Oak Ridge National Laboratory for the U.S. Department of Homeland Security