Control system cyber security – a Sandia perspective

SAND2011-8161C

It is what it is...	To better secure control systems, we need...	Because of this, Sandia's...
• Control system applications, devices, protocols, and architectures are ubiquitous across critical infrastructure • COTS hardware, software, and communications increase the attack landscape in terms of available information and known vulnerabilities • Adversaries are starting to show interest in lower-level devices and networks • Top priority is availability, not security	• tools purpose-built for control system analysis • defense-in-depth systems purpose-designed for control system protocols and transports • policies and procedures purpose-driven towards protecting against, responding to, recovering from, and operating through cyber attacks • operators with increased knowledge about cyber vulnerabilities and attack vectors	• developing assessment tools and techniques safe for use on critical infrastructure • conducting control system and device assessments at and for sites of interest • developing malware analysis, forensics, and out-of-band situational awareness tools specific to control system HW, SW, network transports, and protocols • modeling control systems and industrial processes in support of vulnerability analysis and security testing • training security experts how to safely conduct control system assessments and operators how to recognize cyber attacks

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.