CS²SAT
Control System Cyber Security Self-Assessment Tool

Homeland Security

CONTROL SYSTEM CYBER SECURITY SELF-ASSESSMENT TOOL

Purpose

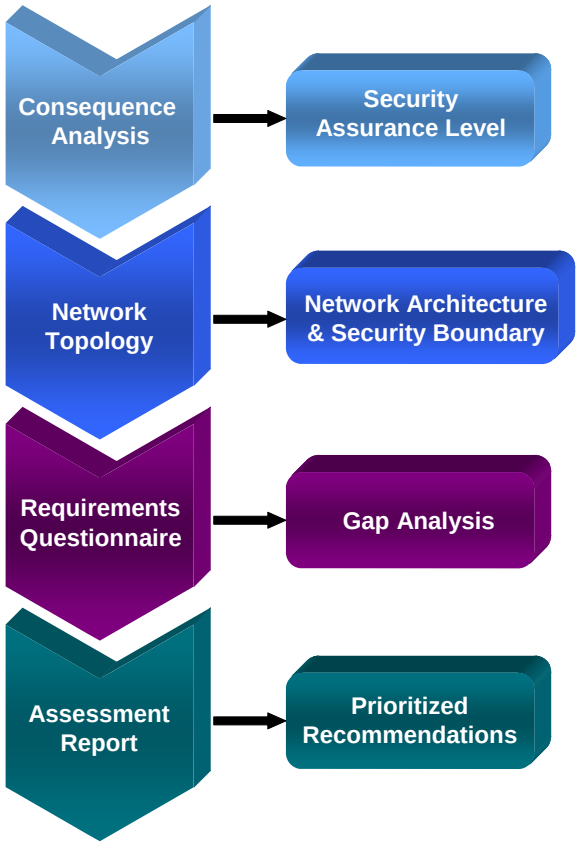
The Control System Cyber Security Self-Assessment Tool (CS²SAT) provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system network. The CS²SAT was developed under the direction of the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) by cyber security experts from national laboratories and with assistance from the National Institute of Standards and Technology. The CS²SAT is a desktop software tool which guides users through a step-by-step process to assess their control system network against recognized security standards. The tool then makes prioritized recommendations for improving the network's cyber security defenses. The tool derives its recommendations from a database of cyber security practices, which have been adapted specifically for application to industry control system networks and components. Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities.

How it Works

The CS²SAT has four functional elements that perform as follows (see the Functional Element diagram):

Consequence Analysis helps the user analyze the criticality of a site or facility relative to the potential negative consequences of a successful cyber attack. This element contains a questionnaire to assist the user to determine the potential losses that could occur from a compromised control system in terms of economic losses, death or injury, and environmental impacts. Once the user has responded to a series of questions, the Consequence Analysis element calculates a recommended minimum security assurance level (SAL) for the facility or subsystem. The SAL indicates the recommended level of rigor needed to protect against the anticipated consequences of a compromised system.

CS²SAT Functional Elements



Network Topology helps the user identify the network architecture and components that are critical to the system's cyber security boundary and posture. This element contains a graphical user interface, which allows the user to load the control system network topology (including criticality levels) into the tool's software. An icon palette is provided for the various system components and the application allows the user to drag and drop the components into a representative diagram.

Requirements Questionnaire generates a set of questions based on the specific *Network Topology*, *Consequence Analysis,* and the security standards which the user selects for comparison. The tool guides the user through the questions and the user selects the best answer to each question, based on the control system's configuration and specific security polices and practices. The tool compares the user's answers with the recommendations for the selected security standards and assurance level. Security gaps are then identified between the user's control system configuration and the recommended practices to meet the selected standards.

Assessment Report provides a prioritized list of control systems security recommendations from the results of the questionnaire. The recommendations provide the user with a systematic approach to address control systems security improvements based on the greatest potential to reduce the risk of a successful cyber attack. A graphical representation of the analysis is also provided so the user can easily identify areas that need improvement.

Homeland Security

CS²SAT Version 1.0.1

Version 1.0.1 of the tool was recently released and is now available on compact disc through licensed distributors. CS²SAT distributors are listed on our website at:

www.us-cert.gov/control_systems/

Agencies which manage and operate federally owned facilities may obtain and use the CS²SAT at no cost. To obtain a copy please send an email to:

cssp@dhs.gov

The Department of Homeland Security CS²SAT team has collected and assembled a comprehensive set of cyber security recommendations based on the best available and emerging standards in the control system community. This information is incorporated into the tool's software, which provides a user-friendly desktop or laptop interface for users to systematically retrieve requirements specific to their control system network.

If you are interested in learning more about the DHS Control Systems Security Program (CSSP) and its efforts to improve cyber security within the Nation's critical infrastructure, please visit our website or send us an email to the location listed above.

Department of Homeland Security

The Homeland Security Act of 2002 provides the basis for the Department of Homeland Security's (DHS) responsibilities in the protection of the Nation's Critical Infrastructure/Key Resources (CI/KR). The National Cyber Security Division (NCSD) of DHS works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To protect the cyber infrastructure, NCSD has identified two overarching objectives: to build and maintain an effective national cyberspace response system and to implement a cyber risk management program for protection of critical infrastructure.

The goal of the Control Systems Security Program (CSSP) is to reduce cyber risk to critical infrastructure control systems by providing guidance, building partnerships, and preparing to respond to incidents. To reduce the risks of a cyber attack on control systems in the CI/KR sectors, the DHS CSSP is partnering with Federal, State, local, and tribal governments and control systems owners, operators and vendors.

Contact Information

Email: cssp@dhs.gov