



Homeland Security

Control Systems Architecture Analysis Services

Design Architecture Review

The Industrial Control System Cyber Emergency Response Team's (ICS-CERT) Design Architecture Review (DAR) provides critical infrastructure asset owners and operators with a comprehensive technical review and cyber evaluation of the architecture and components that comprise their industrial control systems (ICS) operations.

This 2-3 day review includes a deep-dive analysis of the operational process - focusing on the underlying ICS network architecture, integration of Information Technology (IT) and Operational Technology teams,

Because ICS-CERT's DAR is based on Congressional funding, it is available as an onsite facilitated assessment for critical infrastructure asset owners and operators at no cost. Upon completion of the process, ICS-CERT will compile an in-depth report for the asset owner, which includes a prioritized analysis of key discoveries and practical mitigations for enhancing the cyber security posture of the organization. All information shared with ICS-CERT during the analysis and the report outcomes are confidential to the asset owner and protected by DHS as Protected Critical Infrastructure Information (PCII). To schedule an assessment, please contact ICS-CERT at ics-assessments@hq.dhs.gov.

vendor support, monitoring, cyber security controls, and all internal and external connections.

ICS-CERT's assessment team works interactively with your IT and operations personnel to evaluate the current architecture and processes, with focus on three key areas:

1. ICS Network Architecture

- Perimeter defenses (both ingress and egress)
- Remote access methods
- Device to device communications (including protocols)
- Field device communications (wired and wireless)
- Trust relationships and interconnectivity with the enterprise network
- ICS protocols and methods of communication (wired and wireless)

2. Asset Inventory

- Network and field devices for known vulnerabilities and potential exploitation vectors
- Configuration baselines and conformance to industry best practices and hardening guidelines
- Configuration backup and recovery
- Vendor management and integration
- Data and information integrity
- Physical security of critical assets

3. Protective and Detective Controls

- Technologies and methods utilized for detecting anomalous activities
- Review of network device configurations
- Monitoring and alerting mechanisms and processes
- Threat and intelligence data sources – and how these are leveraged within the ICS environment



Homeland Security

Network Architecture Verification and Validation

ICS-CERT's Network Architecture Verification and Validation (NAV) is a passive analysis of network traffic occurring within the ICS network.

Using a combination of both open-source and commercially available tools, ICS-CERT is able to present a strategic visualization of the network traffic and device-to-device communications that are occurring within ICS network segments.

ICS-CERT's assessment team works interactively with your IT and Operations personnel to evaluate the captured network traffic, reviewing:

- Protocol hierarchy and organization of network traffic
- Device to Device communications – including identification of “top-talkers” and the devices generating the most traffic
- Communications traversing (or attempting to traverse) the ICS network boundary – for verification that the perimeter protections are functioning as intended
- Potentially misconfigured devices – or those exhibiting suspicious or anomalous behavior
- ICS protocol analysis - including an in-depth review of function codes and control parameters that are observed within the captured traffic.

Baselining Network Traffic

This service offering provides asset owners with a practical method for baselining network traffic occurring within their ICS network segments. This equates to a powerful detection mechanism to identify abnormal or suspicious traffic occurring within the control environment.

Outcomes

ICS-CERT will compile an in-depth and detailed report for the asset owner upon completion of the process. In addition to the analysis, ICS-CERT provides an overview of the tools utilized – and conducts interactive training on how to best utilize the analysis tools. The ICS-CERT NAV is also available to critical infrastructure owners

and operators at no cost. Like the DAR, all information shared with ICS-CERT during the analysis and the report outcomes are confidential to the asset owner and protected as PCII.

About ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), within the Department of Homeland Security's (DHS) National Protection and Programs Directorate's Office of Cybersecurity and Communications and National Cybersecurity & Communications Integration Center (NCCIC), works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, tribal, and territorial governments and control systems owners, operators, and vendors.

For more information, please go to:

www.ics-cert.us-cert.gov.

About DHS Cyber

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information, please visit

www.dhs.gov/cyber.