

# Non-obtrusive Authentication of Critical Infrastructure Operators (NACIO)

*Hardening security for existing PCS Networks*



## Overview

NACIO addresses a large security hole that exists in many critical infrastructure control centers. Because of operational constraints, operators are not authenticated to the workstations that control critical infrastructure. Anyone with physical access to the workstation has the ability to issue commands and control the critical systems. NACIO provides mechanisms to detect and track critical commands and tie them to the issuing operator in a transparent manner.

## Key Features and Benefits

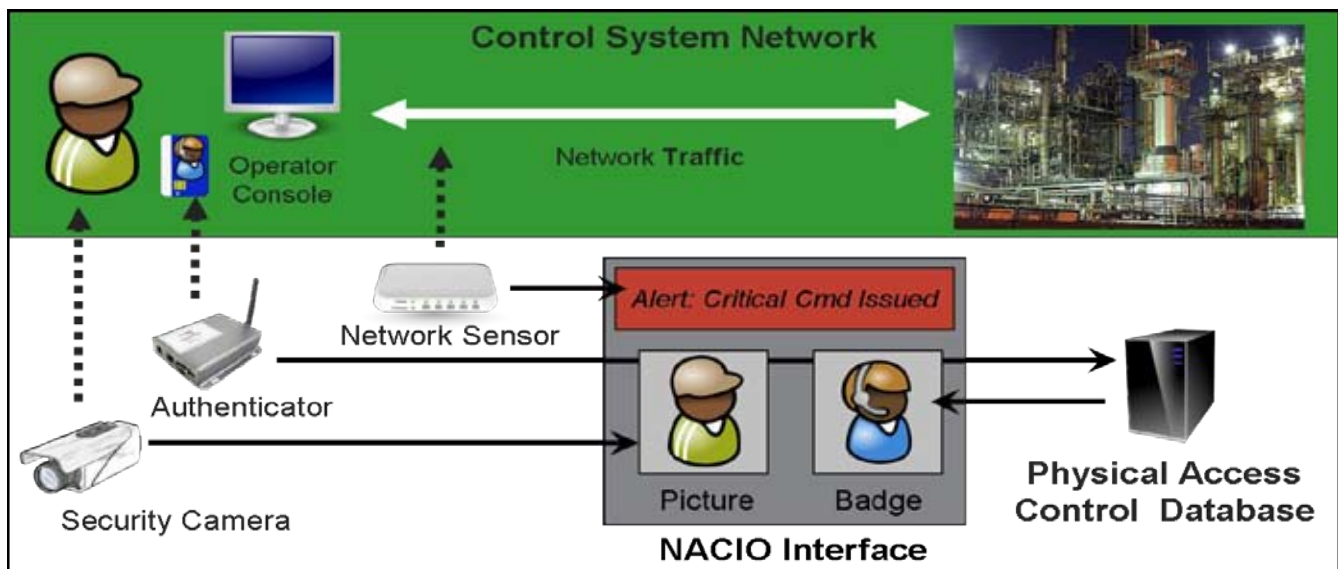
- Provides audit records
- Minimal to no impact on existing networks
- Meets operational, regulatory and cyber security requirements
- Is transparent to the users
- Can detect remote control of workstations
- Minimizes quantity of logs

## Why Authentication is Hard?

Today's cyber and regulatory environment are calling for more stringent auditing of who accesses critical systems and what actions are performed on these systems.

On the other hand potential emergency situations in industrial control systems require immediate access to operator workstations. Typical authentication mechanisms, i.e. username and password, have the possibility, however small, of preventing an authorized operator from using the workstation to prevent or respond to an emergency which could lead to loss of life. To mitigate this possibility most control system workstations are always on and available.

How can both regulatory and operational constraints be met? NACIO is one solution to this challenging problem.



Conceptual View of NACIO



Researchers at Pacific Northwest National Laboratory are advancing the frontiers of scientific knowledge and rapidly translating their discoveries into innovative technologies. State-of-the-art facilities combined with innovation and creativity help Pacific Northwest's scientists and engineers resolve critical challenges in energy, the environment, and national security for government and industry clients. Pacific Northwest also strives to move scientific gains from the laboratory to the marketplace through various programs and partnerships.

## Functional Description

NACIO bridges the gap between standards/regulations and operational needs by using COTS products and some customization to provide a method to authenticate critical infrastructure operators.



**Passive:** The passive version of NACIO creates an audit trail of critical commands, a photo of the operator that issued the command, details of the actions, and the credentials of the operator.

**Active:** The active version of NACIO adds authentication to the passive version. With this version critical commands can only be issued to the control system if an authorized user is present at the issuing workstation.

## Technical Description

NACIO utilizes COTS products for the network sensor, camera and authentication mechanism. By combining them in a novel way it is possible to track control center operators without impacting the network or requiring extra effort by the operators.

NACIO monitors Modbus/TCP traffic and triggers alerts on specific commands. These activate a number of sub-systems to collect badge info, a snapshot at the workstation, and a copy of the network traffic causing the alert. All this information is then correlated and stored for later examination. This information can then be displayed in a stand alone system or integrated into existing security tools.

The ability to block unauthorized commands is also possible.

## Summary of Costs

	Low	Medium	High
Component	<\$1,000	\$1,000-\$10,000	>\$10,000
Engineering	Drop-in	Moderate Modification	Complete System Design Lifecycle
Bandwidth/Network Burden	None-Passive Only	Moderate Traffic Medium Overhead	Heavy Traffic Large Overhead
Training	No Training Required	Moderate Training	Intensive Training Additional Staffing may be required
Maintenance and Operation	< 1 hour per week	< 5 hours per week	> 5 hours per week

## Technology Transfer and Readiness:

The majority of the components that make up NACIO are commercially available tools. The security monitor and security appliance have been bench tested.

Component	Readiness
Network Camera	Commercially Available
Authentication Mechanism	Commercially Available
Location Server	Commercially Available
Security Appliance	Bench Tested
Security Monitor	Bench Tested

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Numbers 2006-CS-001-000001 and 2003-TK-TX-0003, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

**Researcher Contact Information**  
 Sam Clements [samuel.clements@pnl.gov](mailto:samuel.clements@pnl.gov)  
 Mark Hadley [mark.hadley@pnl.gov](mailto:mark.hadley@pnl.gov)



The I3P is managed by Dartmouth College.