

# NACIO

## Non-obtrusive Authentication of Critical Infrastructure Operators

Samuel Clements  
*Pacific Northwest National Laboratory,*  
*Richland, WA 99352*  
[Samuel.Clements@pnl.gov](mailto:Samuel.Clements@pnl.gov)

Thomas Edgar  
*Pacific Northwest National Laboratory,*  
*Richland, WA 99352*  
[Thomas.Edgar@pnl.gov](mailto:Thomas.Edgar@pnl.gov)

### Abstract

*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 control these critical systems. NACIO provides mechanisms to detect and track critical commands and tie them to the issuing operator in a transparent manner.*

### 1. Introduction

Traditional authentication mechanisms are inadequate for many workstations that control real-time process control systems. Loss of access to these workstations can result in catastrophic events including the loss of life. The time required for operators to remember strong secure passwords during situations of high stress like a catastrophic event or even the few minutes required to log off and log on are considered unacceptable.

The control rooms that physically house these workstations are occupied by multiple, often many, people who can make changes to any system. The authentication and logging systems commonly in use today are the badged access logs created when a user enters the physically secured area and a paper log located at the workstation that the operator is supposed to fill out when changes are made to the control system. A utility will know who is in the control room but there is currently no automated way to identify the specific person who issues a command.

The challenge is to devise a method to identify and authenticate users without requiring the system be locked or otherwise unavailable for any period of time. NACIO attempts to do this using a novel approach and integrating commonly available tools and technologies.

NACIO takes advantage of the fact that the networks used to control industrial systems are quite static compared with traditional information technology networks. Nodes on an industrial control system (ICS) communicate only with specific nodes and the communication is very repetitive and predictable. An IT system workstation, on the other hand, may communicate with many nodes one day and entirely different nodes on different protocols the next day. Our approach capitalizes on the static nature of the ICS.

### 2. Phased Approach

Control center workstations control critical equipment that run physical processes. Often these processes can be dangerous and/or provide life critical services and must be managed under very high reliability and safety constraints. Therefore, equipment that is used in these systems must be well tested and proven to not have a negative impact that oversteps these bounds. NACIO is being developed in two phases to accommodate the high reliability requirements of this environment.

#### 2.1 Phase 1 - Passive Monitor

The initial phase places a passive network monitor in the ICS that triggers on critical commands. These commands can be user defined but typically would be ones that modify the normally static environment. Once a critical command is detected a number of mechanisms are activated to identify the initiator of the command. These mechanisms will be discussed in section three. Once the identity of the initiator is known it is logged and available for auditing and forensic purposes. If no one is found to be present during the issuance of the critical command, an alert is logged to warn security staff that an unauthenticated command was sent. Investigation

into the logged information could assist in detecting malicious software presence.

## **2.2 Phase 2 – Active Authentication**

Once phase one is proven to reliably and accurately identify the initiator of an event, phase two will place an active monitor inline with the ICS communication media. The inline sensor will act as a filter of critical commands. When a critical command is received NACIO will use the same authentication mechanisms described in phase 1 and which are defined in section three. If the person present authenticates and has access rights for executing the critical command then the command is sent through to the remote device. Otherwise, NACIOS blocks the command from achieving its destination and logs an alert.

## **3. Identification Mechanisms**

A number of identification mechanisms exist and none are foolproof. NACIO utilizes multiple mechanisms to create a robust identification system.

### **3.1 Networked Security Camera**

A networked security camera is placed to monitor each workstation within a control center. The camera is triggered by the monitor when a critical command is detected and takes a picture of the triggering workstation. These cameras must be placed such that they are not easily blocked and provide a clear view of the person(s) at the workstation. The photos provide an audit trail and provide useful forensic evidence in the event of an investigation.

### **3.2 Passive RFID Tags**

Most control centers have physical access control. This is most frequently done using a badge with embedded radio frequency identification (RFID) chip and readers at entry points to the control room. NACIO has been tested using RFID tags and been able to read them, with varying rates of success, while the user is seated at a workstation. There are a number of variables that affect the accuracy of the system; the tag reader, the angle of the tag relative to the reader, the physical properties of the environment and the body type of the operator all seem to have an effect.

### **3.3 Active Wifi Tags**

Active Wifi tags differ from passive tags in that they have their own power source. It is expected that the difficulty of reliably reading passive tags will not be as significant a challenge with active tags. The challenges we foresee with this technology is the battery life of the tags and difficulty of integrating the technology. There are different techniques to determine location with active tags; Time difference of arrival (TDoA) and received signal strength indication (RSSI) are the two most common. Our initial testing showed that neither of these achieves the location accuracy necessary to uniquely identify a user to a workstation. Another technology that is available and merits more research is choke point technologies which claim to obtain the higher resolution required. Choke points are devices that can be placed at specific location and cause the tags to beacon with advertised accuracy from three inches to six feet.

### **3.4 Facial Recognition**

NACIO takes a picture of the operator so naturally facial recognition would be an excellent identifier. We hope to be able to research this further but our initial research indicated that the number of variables that need to be overcome to get an accurate read from a distance is sufficiently difficult that we looked to other technologies first.

### **3.5 Bluetooth**

In today's highly connected world nearly everyone has a cellular phone. Bluetooth is a common feature on many of these phones and we propose that using the pairing capability of Bluetooth devices could be an easy and effective way to identify a user when they are in proximity of a given workstation.

### **3.6 Facial Detection**

NACIO takes a photo whenever it detects a critical command. Facial detection software would automatically identify if a human was present when that command was issued. This helps detect remote access and possibly compromised machines. This area needs more research.

### **3.7 Other Mechanisms**

NACIO could incorporate many other identification mechanisms depending on cost and practicality. We could look at millimeter wave technologies, iris scans, or other biometric identifiers.

## **4. Results**

This project has a functioning proto-type on which we have begun to test the various mechanism described above. This section details the results of these tests.

### **4.1 Active Wifi Tags**

The preliminary studies into the location resolution of active tags determined that on average the location of the tag could be determined with in a 16 foot radius. This testing was performed using RSSI and between 10 and 20 location receivers. We are currently studying the battery life of the active tags when used in conjunction with choke points.

### **4.2 Passive Tags**

Results from different types of passive RFID tags provided drastically different results. The Alien 9540 Squiggle tag had the best results for our application but is still was not reliably read. Devising tests to evaluate single variables with repeatable results have proven difficult.

## **5. Challenges**

The principle challenge this research is attempting to address is the need to identify and authenticate users of critical infrastructure workstations in such a manner as not to impact the operational requirements of this industry.

The technical challenges are integrating many disparate technologies into one system, getting the resolution necessary to uniquely identify who is in proximity to a given machine when a critical command is issued using the technology available and ultimately refining the system to be reliable and accurate enough for industry to accept and implement it.