

The Integration of Biometric Technologies with Fire Fighting Information Systems

Jan Guynes Clark
Alexander McLeod
Darrell Carpenter

The University of Texas at San Antonio

Overview

- Background
 - Problem Description
 - Proposed Biometric Solution
 - Research Partners
 - Goals
- Status
 - Progress to date
 - Problems Encountered
 - Lessons Learned
- Summary

Problem Description

- San Antonio Fire Department identified three major areas for improving incident response:
 1. Reliable tracking of who is on duty
 2. Managing firefighters responding to an emergency site
 3. Maintaining accurate incident response data

Reliable Tracking

1. Current system

- Company officer inputs list of people working at shift change

2. Problems

- Tradition of informal “Trading time” complicates process
- Updating system when people change out during shift

Managing Firefighters

Responding to an Emergency Site

- Current system
 - White boards
 - Velcro badge system
- Problems
 - Restricts operations to single point of entry
 - Doesn't allow identification of full set of responder qualifications
 - Doesn't scale well for larger incidents
 - Recipe for tactical decision errors

Maintaining Accurate Incident Response Data

- Current system
 - Maintains record of units (not individuals) responding created by Computer Aided Dispatch System
- Problems
 - Doesn't identify individuals on unit
 - Difficult to positively reconcile incident data with individual responders
 - Inefficient long-term management tool
 - Health monitoring
 - Legal liability

Proposed Biometric Solution

- Place biometric fingerprint readers on apparatus and station PCs
 - Fire fighters will authenticate to prove they are who they claim to be
- Integrate authentication information with electronic incident command system via existing wireless network
 - Deliver real-time unit and personnel data to incident commander in the field

Biometric Solution – Potential Benefits

- Positive firefighter authentication – individual must be present to authenticate
- Leverage strong “tradition” that assigned positions always deploy with apparatus
 - Not shift related – can be verified anytime - even enroute

Biometric Solution – Potential Benefits (cont.)

- Potential for extended capability
 - Management of “trading time” limits
 - Enforcement of policies – ie. what rank / qualification can fill position
- Can provide real time unit/individual data on multiple displays simultaneously
 - Does not restrict operations to single point of entry
- Shows units, on-scene, enroute, dispatched
- Highly scalable

Biometric Solution – Potential Benefits (cont.)

- Additional Synergies
 - Authentication complements, rather than replaces other locating / tracking technologies
 - Can provide detailed personnel qualifications with links to additional existing systems
 - Swift water rescue, High angle technical rescue, etc.
 - Facilitates health monitoring, matching of incident/individual responder data
 - Appears well-suited to regional / multi-agency implementations
 - Incident commander can reliably trust authenticated persons
 - Can verify their qualifications

Research Partners

- San Antonio Fire Department
 - Deputy Chief of Operations
- San Antonio Information Technology Dept.
 - CIO, IT managers
- University of Texas at San Antonio
 - IT Researchers, students
- Salamander Technologies
 - Executive Vice-President

Goals of Pilot Study

- Proof-of-concept
 - Demonstrate that the integrated biometric / incident command system is feasible
 - Assess realization of projected benefits
 - Identify potential weaknesses & mediation steps
 - Recommend policies & procedures

Assess User Reactions

- Measure privacy concerns related to system
 - Accountability
 - Will users fear a higher level of accountability if they use a biometric?
 - Trust
 - Will users trust the organization not to use biometric data for undisclosed purposes?
 - Vulnerability
 - Do users believe the organization can keep their biometric data safe from hackers?

Status - Completed:

- Procured necessary equipment
- Tested individual system components
- Developed biometric privacy instrument and conducted focus group review
- Installed and tested biometric server

Status - Next steps:

- Validation of privacy instrument using fire fighters
- Installation of biometric devices on station PCs and apparatus
- Deployment of incident command software
- Testing of end-to-end system

Problems Encountered

- Changes in vendor product offerings
 - Specified file server discontinued
 - Waited for city to release new “standard server” specifications to ensure reliability
 - Biometric sensors discontinued
 - Slight changes in sensors due to manufacturer changes

Problems Encountered

- Key personnel changes
 - Hiring of new City Manager, Fire Chief, and CIO
 - Departure of Salamander Technologies lead developer
 - Promotion / reassignment of Fire Department's lead IT programmer

Problems Encountered

- Change in Incident Command product
 - Original proposal was designed to integrate with a locally developed incident command application
 - The city later decided to purchase the commercial Fire Trax program
 - It made sense from grant perspective to integrate this new system rather than continue with original plan

Lessons Learned

- Biometrics is dynamic field
 - Need wide vendor support to avoid obsolescence
- High-level buy-in is paramount
- Learn to deal with resistance to change from unexpected sources

Summary

- System development has progressed largely as planned
- Although changes in hardware availability, key personnel and the incident command software have caused some schedule slippage to occur, we still expect the system to be operational by summer