US Department
of Transportation

**Federal Railroad
Administration**

Research Results

**RR 08-23
October 2008**

Development of a Locomotive Security System Using Biometric Authentication

SUMMARY

The Federal Railroad Administration's (FRA) Office of Research and Development has developed a biometric-based Locomotive Security System (LSS) to evaluate as a mechanism to prevent unauthorized use of locomotives. The project's main objective is to improve railroad safety and security using advanced technologies.

The LSS integrates available off-the-shelf biometric and ID card reader technologies into a rugged enclosure for application in the harsh railroad environment. The system is easy to use and provides business benefits beyond locomotive safety including:

- logging and tracking of locomotive crew operating times,
- positive identification of train operators at any moment in time, and
- validation of operator against event recorder data for crew-based incentives and incident investigations.

One system has been installed and operational on the FRA Advanced Concept Train (ACT) locomotive for over a year. Additional LSSs will be installed and monitored on two of TTCI's locomotives at Pueblo, Colorado, in 2008.

Figure 1 – Locomotive Security System Hardware

BACKGROUND

Locomotive and train cargo security has been a concern of railroad operations for many years. FRA initiated the research into the development of an LSS after the events of September 11, 2001, and the Madrid train bombings on March 11, 2004. These incidents proved that today's transportation systems are vulnerable to terrorist attacks.

During this period, the U.S. Department of Transportation evaluated its transportation system to determine vulnerable areas that could benefit from enhanced security. Today's locomotives have very limited protection to prevent unauthorized users from gaining access and control of a train. Thus, one area of concern was the possibility of an unauthorized person overtaking a train containing hazardous materials and intentionally derailing it or taking other actions to cause a hazardous chemical spill in a densely populated area.

This research investigates the feasibility of using biometric-based authentication devices as an effective and reliable technology for securing today's locomotives. Biometric technology is widely used throughout the industry, from access control of the U.S. Department of Defense highly secured areas to entry into the Walt Disney World theme parks. It validates the identity of an individual by examining certain unique characteristics. Biometric devices compare an input sample (such as a fingerprint) to a previously stored template to determine if a match is present.

OBJECTIVES

The main objectives of this project were to:

- Determine if biometrics can be used effectively and reliably in the rugged railroad environment as a mechanism to verify the locomotive operator identity (authentication).
- Demonstrate the ability of the LSS to prevent locomotive movement, and for a remote central dispatch location to grant permission for a railroad employee to operate a locomotive at a specific time and location (authorization).
- Demonstrate the ability of the LSS to function as a replacement to the alerter system currently used to validate that the operator is alert, vigilant, and in control of the train.

METHODS

To prevent unauthorized users, the identity of the individual attempting to operate the train must be determined. There are three types of identifying factors:

- Something you **have** (possession-based) using one specific "token" such as an ID Badge, Smart Card, or Key,
- Something you **know** (knowledge-based) such as Personal ID Number (PIN), Password, or User ID
- Something you **are** (biometrics) such as fingerprint, iris scan, or voice recognition.

The LSS design incorporates a combination of at least two of these factors to confirm the identity of the operator.

The LSS design uses commercial-off-the-shelf (COTS) hardware whenever possible. The biometric and card reader technology incorporated in this design is commonly used in building access control and has been proven to withstand harsh environmental conditions. The ID card technology implemented is standard with many railroads and other companies, allowing one card for corporate ID and locomotive security access.

Privacy and security are often a concern when implementing biometric technologies. The fingerprint data are encrypted using the same secure technology as the Department of Homeland Security has specified for use in its Transportation Worker Identification Credential (TWIC) cards [1]. The LSS can be configured to store the encrypted fingerprint data in any of the following configurations:

- only on the ID card to maximize employee control of their identifying information,
- in an employer database so that an employee does not need to carry an ID card with them, and
- both on the card and in the database.

To support the onboard authentication and authorization process, the locomotive cab is equipped with a wireless computing platform and a rugged LCD touch screen. The computing platform is Wi-Tronix's Wireless Processing Unit, or Wi-PU. The Wi-PU is a proven device used in hundreds of locomotives throughout North America. The Wi-PU's software manages all communications with the LSS hardware, handles the locomotive interface that prevents locomotive movement, and implements the graphical user interface that displays the current state of the locomotive to the operator. The user interface incorporates railroad industry standard formats [2] to provide the operator with easy to follow actions required to enable locomotive movement.

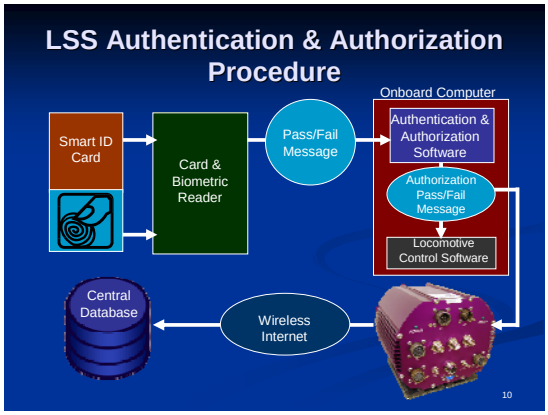

Figure 2 – LSS Overview

RESULTS

Biometric technologies from different fingerprint readers were evaluated based on several factors including cost, accuracy, interface capabilities, and ability to operate in harsh environments. The prototype LSS incorporates a rugged and reliable fingerprint reader with a standard ID card reader into an integrated enclosure (Figure 1).

The LSS secures the locomotive in a 'locked' state by preventing locomotive movement until an operator has been authenticated and authorized to move it. The overall LSS authentication and authorization process is shown in Figure 2.

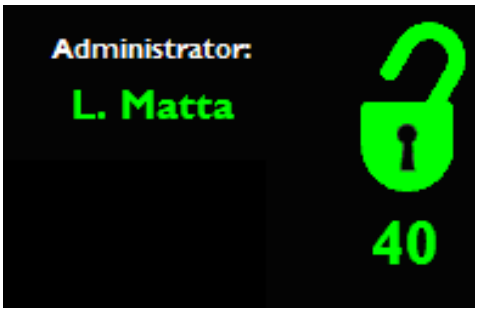

Figure 3 – LSS User Interface

Authentication is granted when identity is confirmed through a combination of an ID card and a fingerprint. The LSS device reads the fingerprint presented by the operator and compares it with the previously stored fingerprint read from the smart ID card. If there is a match, authentication is successful and the LSS retrieves and searches a list of authorized users for that locomotive. If the operator identity is verified and authorization is successful, the locomotive is 'unlocked' and ready for movement.

Figure 3 shows a portion of the LSS user interface when the locomotive has been 'unlocked.' The name of the current authorized operator is displayed along with a green icon indicating that the system is unlocked and ready for use. When the locomotive is 'locked' a red lock is displayed and no operator name is present.

Authorization levels are configurable as the system is deployed to enable greater levels of security. An authorized railroad representative grants an authorization for locomotive operation from a central dispatch center via a web interface. In a minimum security authorization configuration, all employees can access all locomotives at any time and location. In a maximum security authorization configuration, an individual operator can only operate specific locomotives at a specific time and location. The authorization can be revoked at any time using the same web interface. The locomotive periodically downloads and validates the operator against the latest authorization information.

Figure 4 – Sample LSS Application on ACT

The LSS requires the operator to periodically reauthenticate to ensure that they are alert and actively operating the train. The timing of the reauthentication logic is based on the existing locomotive alerter/vigilance system, in which the rate of required operator input varies depending on the speed of the train. If the operator fails to reauthenticate before the timer expires, the LSS will automatically apply the brakes in a manner similar to the existing alerter system. This makes the LSS more secure than the alerter system by also verifying the identity of the locomotive operator to allow continued operation. The LSS also incorporates a silent alarm feature.

CONCLUSIONS

A pilot Locomotive Security System has been developed, validated and installed on FRA's Advanced Concept Train (Figure 4). The system is cost-effective and incorporates existing technologies in a new and different application. The use of biometric technology in the railroad environment is ongoing and will be evaluated as the locomotive continues operation in revenue service.

FUTURE ACTION

Additional pilot deployments of the locomotive security system are planned for 2008. These pilots will focus on the business efficiency benefit of the system. These benefits complement the core purpose of LSS: to improve rail security and safety.

ACKNOWLEDGEMENTS

The Locomotive Security System was developed by Wi-Tronix, LLC under direction of the FRA as part of the Advanced Concept Train.

REFERENCES

[1] http://www.dhs.gov/xnews/releases/press_release_0558.shtm

[2] "AAR Manual of Standards and Recommended Practices for Railway Electronics, Specification M-591: Operating Display", Association of American Railroads, 2004

CONTACT

Monique F. Stewart
Shahram Mehrvarzi
John Punwani
Federal Railroad Administration
Office of Research and Development
1200 New Jersey Avenue SE - Mail Stop 20
Washington, DC 20590
(202) 493-6358 [Monique]
(202) 493-6108 [Shahram]
(202) 493-6369 [John]
monique.stewart@dot.gov
shahram.mehrvarzi@dot.gov
john.punwani@dot.gov

KEYWORDS

locomotive, biometric, wireless, communi-cations, monitoring, gui, smart card, security, railroad, hazardous materials